aws

Benutzer-Leitfaden

Amazon Elastic VMware Service

Amazon Elastic VMware Service: Benutzer-Leitfaden

Table of Contents

Was ist Amazon Elastic VMware Service?

Sie können Amazon Elastic VMware Service (Amazon EVS) verwenden, um eine VMware Cloud Foundation (VCF) -Umgebung direkt auf EC2 Bare-Metal-Instances innerhalb Amazon Virtual Private Cloud (VPC) bereitzustellen und auszuführen.

Themen

Funktionen von Amazon EVS

Im Folgenden sind die wichtigsten Funktionen von Amazon EVS aufgeführt:

Vereinfachen und beschleunigen Sie Ihre Migration zu AWS

> Beseitigen Sie Probleme bei der Migration und sorgen Sie mit der Abonnement-Portabilität und der automatisierten Bereitstellung von VMware Cloud Foundation (VCF) in der Cloud für einen konsistenten Betrieb. Erweitern Sie lokale Netzwerke und migrieren Sie Workloads, ohne IP-Adressen ändern, Mitarbeiter umschulen oder betriebliche Runbooks neu schreiben zu müssen.

Behalten Sie die Kontrolle über Ihre Architektur in der Cloud VMware

> Behalten Sie die vollständige Kontrolle über Ihre VMware Architektur und optimieren Sie einen Virtualisierungs-Stack, der die individuellen Anforderungen Ihrer Anwendungen erfüllt, einschließlich Add-Ons und Lösungen von Drittanbietern.

Managen Sie sich selbst oder nutzen Sie AWS Partner für ein gemanagtes Erlebnis

> Nutzen Sie die Wahlmöglichkeiten und Flexibilität bei der Selbstverwaltung oder nutzen Sie das Fachwissen von AWS Partnern für die Verwaltung und den Betrieb Ihrer VCF-Umgebung, AWS um Ihre Geschäftsziele in Bezug auf Talent, Zeit und Kosten zu erreichen.

Skalieren Sie Ihr Unternehmen und schützen Sie es vor Störungen

Verbessern Sie die Skalierbarkeit in der sichersten, skalierbarsten und widerstandsfähigsten Cloud für die Migration und den Betrieb Ihrer Workloads VMware.

Nutzen Sie AWS Innovationen, um Ihre Anwendungen und Infrastruktur zu transformieren

Als AWS-nativer Service vereinfacht Amazon EVS die Erweiterung und Erweiterung Ihrer VMware Umgebung mit mehr als 200 Services (darunter verwaltete Datenbanken, Analysen, Serverless und Container sowie generative KI), um Ihr Unternehmen zu transformieren.

Erste Schritte mit Amazon EVS

Informationen zum Erstellen Ihrer ersten Amazon EVS-Umgebung finden Sie unterErste Schritte. Im Allgemeinen müssen Sie für den Einstieg in Amazon EVS die folgenden Schritte ausführen.

1. Erfüllen von -Voraussetzungen Weitere Informationen finden Sie unter Amazon Elastic VMware Service einrichten.
2. Erstellen Sie eine Amazon EVS-Umgebung. Während der Umgebungserstellung erstellt Amazon EVS die erforderlichen VLAN-Subnetze anhand der von Ihnen angegebenen CIDR-Bereiche und fügt der Umgebung Hosts hinzu.
3. Passen Sie VCF an. Konfigurieren Sie Ihre Umgebung in der vSphere-Benutzeroberfläche entsprechend Ihren Anforderungen. Dies kann die Einrichtung von Logins, Richtlinien, Überwachung und mehr beinhalten.
4. Connect und migrieren. Connect Sie Ihre Umgebung mit Ihrem lokalen Rechenzentrum und migrieren Sie Ihre VCF-Workloads zu Amazon EVS.

Zugreifen auf Amazon EVS

Sie können Ihre Amazon EVS-Bereitstellungen mithilfe der folgenden Schnittstellen definieren und konfigurieren:

- Amazon EVS-Konsole — Bietet eine Weboberfläche zum Erstellen von Amazon EVS-Umgebungen.
- AWS CLI - Stellt Befehle für eine Vielzahl von Programmen bereit AWS-Services und wird unter Windows, MacOS und Linux unterstützt. Weitere Informationen finden Sie unter AWS Command Line Interface.

- AWS CloudFormation - Stellt eine Spezifikation für jeden Ressourcentyp bereit, z. `AWS::EVS::Environment` B. Sie erstellen anhand der Ressourcenspezifikation eine Vorlage und kümmern CloudFormation sich um die Bereitstellung und Konfiguration der Ressourcen für Sie.

Konzepte und Komponenten von Amazon EVS

In diesem Abschnitt werden einige wichtige Konzepte und Komponenten von Amazon EVS erklärt.

Amazon-EVS-Umgebung

Eine Amazon EVS-Umgebung ist ein logischer Container für VMware Cloud Foundation (VCF) - Ressourcen wie vSphere-Hosts, vSAN, NSX und SDDC Manager. Eine Umgebung enthält eine konsolidierte VCF-Domain mit einem vSphere-Cluster, der die Komponenten für Management, Überwachung und Instanziierung des VCF-Softwarestacks hostet. Jede Umgebung ist direkt einer SDDC Manager-Appliance zugeordnet. Weitere Informationen finden Sie unter the section called “Architektur”.

Amazon EVS-Host

Ein Amazon EVS-Host ist ein VMware ESX-Host, der auf Amazon EC2 Bare-Metal-Instances ausgeführt wird. Amazon EVS-Hosts verwenden lokale NVMe Instance-Speicher-Volumes für vSAN-Datenspeicher, in denen Ihre virtuellen Management- und Workload-Maschinen gespeichert werden.

> **Warning**
>
> Instance-Speicher-Volumes sind kurzlebig. Auf diesen Volumes gespeicherte Daten bleiben nicht erhalten, wenn die zugrunde liegende EC2-Instance gestoppt oder beendet wird.
> Das Stoppen oder Beenden von Amazon EC2 Instances, die von Amazon EVS verwendet werden, ohne sie innerhalb von VCF außer Betrieb zu nehmen, kann zu Datenverlust führen.
> Weitere Informationen zur Host-Wartung finden Sie unter. the section called “Host-Wartung”

Subnetz für den Servicezugriff

Das Service-Access-Subnetz ist ein Standard-VPC-Subnetz, das Amazon EVS den Zugriff auf die VCF-Bereitstellung ermöglicht. Bei der Erstellung der Amazon EVS-Umgebung geben Sie die VPC und das Subnetz an, die Amazon EVS für den Servicezugriff verwenden soll.

Wenn Sie eine Amazon EVS-Umgebung erstellen, stellt Amazon EVS elastische Netzwerkschnittstellen im Servicezugriffssubnetz bereit, um die Verwaltungskonnektivität zu VCF-Appliances und ESX-Hosts zu erleichtern. Diese Konnektivität ist erforderlich, damit Amazon EVS die VCF-Bereitstellung bereitstellen, verwalten und überwachen kann.

Amazon EVS VLAN-Subnetz

Ein Amazon EVS-VLAN-Subnetz ist ein Amazon VPC-Subnetz, das von Amazon EVS verwaltet wird. VLAN-Subnetze bieten VPC-Konnektivität für Amazon EVS-Hosts und VCF-Appliances wie VMware NSX, VMware HCX und vCenter Server. VMware Jedes VLAN-Subnetz verfügt über ein VLAN-Tag, mit dem der VLAN-Netzwerkverkehr logisch segmentiert werden kann.

Amazon EVS erstellt alle VLAN-Subnetze, die der Service verwendet, wenn die Amazon EVS-Umgebung erstellt wird. Sie geben die CIDR-Blockeingänge an, die die VLAN-Subnetze verwenden. Sie sollten sicherstellen, dass Ihre VLAN-Subnetz-CIDR-Blöcke entsprechend der Anzahl der zu konfigurierenden Hosts richtig dimensioniert sind, wobei future Skalierungsanforderungen berücksichtigt werden müssen. CIDR-Blöcke müssen eine Mindestgröße von /28 Netmask und eine Maximalgröße von /24 Netmask haben. CIDR-Blöcke dürfen sich nicht mit einem vorhandenen CIDR-Block überschneiden, der der VPC zugeordnet ist.

Bei der Erstellung werden VLAN-Subnetze implizit der Haupt-Routing-Tabelle Ihrer VPC zugeordnet. Nach der Bereitstellung können Sie VLAN-Subnetze explizit einer benutzerdefinierten Routentabelle zuordnen. Weitere Informationen finden Sie unter the section called “Überlegungen zum Amazon EVS-Netzwerk”.

> **Important**
>
> Amazon EVS-VLAN-Subnetze können nur während der Erstellung der Amazon EVS-Umgebung erstellt werden und können nach der Erstellung der Umgebung nicht geändert werden. Sie müssen sicherstellen, dass die CIDR-Blöcke des VLAN-Subnetzes die richtige Größe haben, bevor Sie die Umgebung erstellen. Nach der Bereitstellung der Umgebung können Sie keine VLAN-Subnetze hinzufügen.

> **Important**
>
> EC2-Sicherheitsgruppenregeln werden auf elastischen Netzwerkschnittstellen von Amazon EVS, die mit VLAN-Subnetzen verbunden sind, nicht durchgesetzt. Um den Verkehr zu

und von VLAN-Subnetzen zu kontrollieren, müssen Sie eine Netzwerkzugriffskontrollliste verwenden.

Hostverwaltung, VLAN-Subnetz

Das Host-Management-VLAN-Subnetz trennt den Verwaltungsverkehr vom Benutzerverkehr und ermöglicht die Fernverwaltung von Hosts. Die VMkernel-Netzwerkschnittstelle für die EVS-Hostverwaltung stellt eine Verbindung zu diesem Subnetz her.

vMotion-VLAN-Subnetz

Das vMotion-VLAN-Subnetz segmentiert den VMware vMotion-Verkehr logisch und wird während eines vMotion-Prozesses verwendet, um virtuelle Maschinen zwischen Hosts zu verschieben.

vSAN-VLAN-Subnetz

Das vSAN-VLAN-Subnetz wird von VMware vSAN verwendet, um den Datenverkehr im Zusammenhang mit den Speicheroperationen von vSAN von anderem Netzwerkverkehr zu trennen.

VTEP-VLAN-Subnetz

Das VTEP-VLAN-Subnetz verwendet virtuelle VMware NSX-Tunnel-Endpunkte (VTEP), um den Overlay-Netzwerkverkehr für die Amazon EVS ESX-Hosts zu kapseln und zu entkapseln.

Edge-VTEP-VLAN-Subnetz

Das Edge VTEP-VLAN-Subnetz ist ein spezialisiertes VTEP-VLAN-Subnetz, das für den Overlay-Verkehr der NSX Edge-Appliance vorgesehen ist. Dieses VLAN wird für die Overlay-Kommunikation zwischen NSX Edges und ESX-Hosts verwendet.

VLAN-Subnetz der Verwaltungs-VM

Das VLAN-Subnetz der Management-VM wird für die Verwaltung virtueller Appliances verwendet, einschließlich NSX Manager, vCenter Server und SDDC Manager.

HCX-Uplink-VLAN-Subnetz

Das HCX-Uplink-VLAN-Subnetz wird für die Kommunikation zwischen den HCX Interconnect (HCX-IX) und HCX Network Extension (HCX-NE) Appliances verwendet und ermöglicht die Erstellung des HCX Service Mesh-Uplinks.

NSX-Uplink-VLAN-Subnetz

Das NSX-Uplink-VLAN-Subnetz wird verwendet, um Ihre NSX-Overlay-Netzwerke mit dem Rest Ihrer VPC und allen anderen externen Netzwerken, die Sie konfigurieren, zu verbinden. Das NSX-Uplink-VLAN-Subnetz ist auf den NSX Edge-Knoten-Uplinks konfiguriert.

Erweiterung: VLAN-Subnetz

Das Erweiterungs-VLAN-Subnetz kann verwendet werden, um zusätzliche VCF-unterstützte Funktionen wie NSX Federation zu aktivieren. Amazon EVS erstellt während der Umgebungserstellung zwei Erweiterungs-VLAN-Subnetze.

VMware NSX

VMware NSX ist eine softwaredefinierte Netzwerkplattform (SDN), die Netzwerkvirtualisierung ermöglicht. Amazon EVS verwendet VMware NSX, um das Overlay-Netzwerk zu erstellen und zu verwalten, in dem VMware Cloud Foundation (VCF) -Appliances und -Workloads ausgeführt werden. Amazon EVS stellt ein Paar Active/Standby NSX Edge-Knoten zusammen mit einem NSX-Overlay-Netzwerk bereit. Amazon EVS konfiguriert im Rahmen der Bereitstellung automatisch das gesamte NSX-Routing und die Uplinks in Ihrem Namen. Weitere Informationen zu gängigen NSX-Konzepten finden Sie unter Wichtige Konzepte im NSX-Installationshandbuch. VMware

Konnektor

Ein Amazon EVS-Connector ermöglicht Amazon EVS die Kommunikation mit VMware Cloud Foundation-Management-Appliances, wie z. B. einer vCenter Server-Appliance, in Ihrer Umgebung. Jeder Connector ist einer einzelnen Verwaltungs-Appliance zugeordnet und erfordert den vollqualifizierten Domänennamen (FQDN) und die Anmeldeinformationen, die Sie in einem AWS Secrets Manager-Geheimnis speichern, um sich bei der Appliance zu authentifizieren. Amazon EVS überprüft regelmäßig die Erreichbarkeit der Appliance über den Connector. Wenn der Anschluss nicht mehr erreichbar ist, werden Funktionen, die vom Anschluss abhängen, beeinträchtigt.

- Informationen zum Erstellen eines Connectors finden Sie unter. the section called “Konnektor erstellen”
- Informationen zum Aktualisieren eines Connectors finden Sie unterthe section called “Konnektor aktualisieren”.
- Informationen zum Löschen eines Connectors finden Sie unterthe section called “Konnektor löschen”.

Windows Server-Lizenzberechtigung für Amazon EVS

Mit der Windows Server-Lizenzberechtigung für Amazon EVS können virtuelle Maschinen (VMs), die in Ihrer Amazon EVS-Umgebung ausgeführt werden, AWS angebotene Windows Server-Lizenzen nutzen. Windows Server-Lizenzberechtigungen werden pro vCPU und Stunde mit einem pay-as-you-go Modell angeboten.

Um Windows Server-Lizenzberechtigungen zu verwenden, müssen Sie zunächst einen Connector erstellen, um die Erreichbarkeit zwischen Amazon EVS und Ihrer vCenter Server-Appliance herzustellen. Die Erreichbarkeitsprüfung für den Connector muss bestanden werden, bevor Sie eine Berechtigung erstellen können.

Amazon EVS verwendet den vCenter-Connector, um VM-Lebenszyklusereignisse für berechtigte Benutzer zu überwachen. VMs Wenn der Connector nicht mehr erreichbar ist, gehen die zugehörigen Berechtigungen in den Status „Gefährdet“ über. Wenn die Erreichbarkeit nicht innerhalb einer Nachfrist von 8 Stunden wiederhergestellt wird, werden die Berechtigungen gelöscht und die Nachverfolgung der Lizenznutzung wird ab dem Zeitpunkt beendet, zu dem die Berechtigung den Status „gefährdet“ erreicht hat.

Nachdem Sie eine Berechtigung erstellt und eine VM eingeschaltet haben, beginnt Amazon EVS mit der Überwachung der Windows Server-Lizenznutzung der entsprechenden VM. Wenn die VM heruntergefahren wird oder die konfigurierten vCPUs je nach Bedarf nach oben oder unten skaliert werden, zahlen Sie nur für die Lizenzierung für die gesamten genutzten vCPU-Stunden.

> **Warning**
>
> Unterstützte Gastbetriebssysteme sind Windows Server 2016 und höher.

Anweisungen finden Sie unter the section called “Konnektor erstellen” und the section called “Anspruch erstellen”.

Nachdem Sie Berechtigungen erstellt haben, können Sie jede Windows Server-VM so konfigurieren, dass sie über einen VPC-Endpunkt aktiviert wird. Detaillierte Anweisungen finden Sie unter the section called “Konfigurieren Sie die Windows Server-Aktivierung”.

VMware Hybrid Cloud-Erweiterung (HCX)

VMware Hybrid Cloud Extension (VMware HCX) ist eine Plattform für Anwendungsmobilität, die zur Vereinfachung der Anwendungsmigration, zur Neuverteilung von Workloads und zur Optimierung

der Notfallwiederherstellung in Rechenzentren und Clouds entwickelt wurde. Sie können HCX verwenden, um Ihre VMware basierten Workloads zu Amazon EVS zu migrieren.

Sie können die Konnektivität für VMware HCX mithilfe eines zugehörigen Transit-Gateways oder Direct Connect mithilfe eines AWS Site-to-Site VPN-Anhangs zu einem Transit-Gateway konfigurieren. Weitere Informationen finden Sie unter Migration.

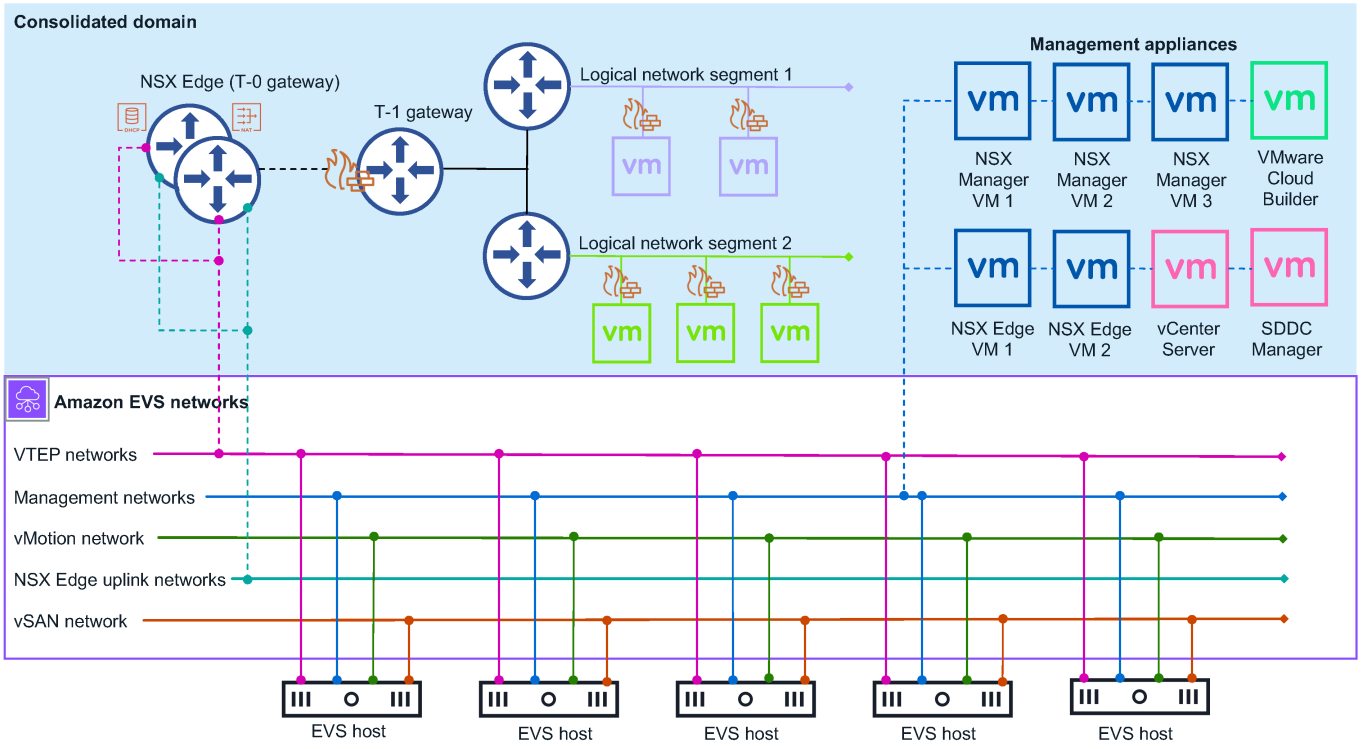
Amazon-EVS-Architektur

Amazon EVS implementiert ein konsolidiertes Architekturmodell der VMware Cloud Foundation (VCF). In diesem Modell werden VCF-Verwaltungskomponenten und Kunden-Workloads zusammen auf einer konsolidierten Domain ausgeführt. Die Amazon EVS-Umgebung wird über einen einzigen vCenter Server mit vSphere-Ressourcenpools verwaltet, die eine Isolierung zwischen Management- und Kunden-Workloads ermöglichen.

Die konsolidierte Domain, die Amazon EVS bereitstellt, enthält die folgenden VCF-Verwaltungskomponenten:

- ESX-Hosts
- vCenter Server-Instanz
- SDDC-Manager
- vSAN-Datenspeicher
- NSX Manager-Cluster mit drei Knoten
- vSphere-Cluster
- NSX Edge-Cluster

Das folgende Diagramm zeigt ein Beispiel für eine Amazon EVS-Architektur, die in einer Amazon EVS-Umgebung bereitgestellt wurde, und zeigt, wie die Komponenten in der Umgebung miteinander verbunden sind. Im Diagramm ist die Amazon EVS-Umgebung mit einer konsolidierten Domain-Architektur blau schattiert. Die zugrunde liegende Amazon EVS-Netzwerktopologie ist in der durchgezogenen lila Linie dargestellt.



Netzwerktopologie

Eine Amazon EVS-Umgebung besteht aus zwei separaten Management-Netzwerkschichten:

Amazon VPC

Die Amazon VPC- und Amazon EVS-VLAN-Subnetze, die während der Umgebungserstellung in der VPC erstellt werden, bilden das Underlay-Netzwerk für Ihre VCF-Bereitstellung. Diese Infrastruktur bietet Konnektivität für NSX-Overlay-Netzwerke, Hostmanagement, vMotion und VSAN. Amazon VPC Route Server ermöglicht dynamisches Routing zwischen dem Underlay-Netzwerk und den Overlay-Netzwerken. Weitere Informationen finden Sie unter the section called “Konzepte und Komponenten”.

> **Note**
>
> Amazon EVS-VLAN-Subnetze werden nur zur Erleichterung der VCF-Underlay-Kommunikation verwendet. Virtuelle Gastmaschinen, auf denen Kunden-Workloads ausgeführt werden, müssen in NSX-Overlay-Netzwerken bereitgestellt werden. Die

Bereitstellung von virtuellen Gastmaschinen im Amazon EVS VLAN-Subnetz-Underlay-Netzwerk wird nicht unterstützt.

VMware NSX-Overlay-Netzwerk

Amazon EVS konfiguriert im Rahmen der Bereitstellung in Ihrem Namen ein NSX-Overlay-Netzwerk. Sie können zusätzliche NSX-Overlay-Netzwerke konfigurieren, um eine Netzwerkisolierung zwischen verschiedenen Workloads oder Anwendungen in Ihrer Amazon EVS-Umgebung zu erreichen. Weitere Informationen finden Sie unter Overlay Design for VMware Cloud Foundation in der VMware Cloud Foundation-Produktdokumentation.

Note

Amazon EVS unterstützt nur ein Tier-0-Gateway für einen Active/Standby NSX Edge-Cluster mit zwei NSX Edge-Knoten. Dieses Tier-0-Gateway stellt eine Verbindung zu allen Overlay-Netzwerken her, die Sie für die Verwendung mit Amazon EVS konfigurieren, und bewirbt diese.

Die beiden Netzwerkschichten sind durch einen Active/Standby NSX Edge-Cluster mit zwei NSX Edge-Knoten verbunden. Die NSX Edge-Knoten ermöglichen die Kommunikation über die VPC zwischen virtuellen Maschinen im Netzwerk VLANs sowie Internetkonnektivität und private Konnektivität über Direct Connect oder AWS Site-to-Site VPN mit einem Transit-Gateway.

Überlegungen zum Amazon EVS-Netzwerk

Das Verwaltungsnetzwerk erfordert die folgenden Netzwerkressourcenkonfigurationen. Sie geben diese Eingaben bei der Erstellung der Amazon EVS-Umgebung an. Weitere Informationen finden Sie unter the section called “Konzepte und Komponenten”.

- Eine Amazon VPC. Stellen Sie sicher, dass Ihr IPv4 VPC-CIDR-Block entsprechend dimensioniert ist, um das erforderliche VPC-Subnetz und die Amazon EVS-VLAN-Subnetze zu berücksichtigen, die Amazon EVS bei der Umgebungserstellung bereitstellt. Weitere Informationen finden Sie unter the section called “Amazon EVS VLAN-Subnetz”.

> **Note**
>
> Amazon EVS unterstützt IPv6 derzeit nicht.

- Ein Servicezugriffssubnetz in Ihrer VPC. Amazon EVS verwendet dieses Subnetz, um eine dauerhafte Verbindung zu Ihrer SDDC Manager-Appliance aufrechtzuerhalten. Weitere Informationen finden Sie unter the section called “Subnetz für den Servicezugriff”.

> **Note**
>
> Amazon EVS unterstützt derzeit nur Single-AZ-Bereitstellungen. Alle VPC-Subnetze, die Amazon EVS verwendet, müssen sich in einer einzigen Availability Zone in einer Region befinden, in der der Service verfügbar ist.

> **Note**
>
> Alle VPC-Subnetze benötigen zugehörige Routing-Tabellen, die gemäß den Netzwerkanforderungen Ihrer Organisation konfiguriert sind.

- Eine primäre DNS-Server-IP-Adresse und eine sekundäre DNS-Server-IP-Adresse im DHCP-Optionssatz der VPC zur Auflösung von Host-IP-Adressen. Amazon EVS erfordert außerdem, dass Sie eine DNS-Forward-Lookupzone mit A-Einträgen und eine Reverse-Lookupzone mit PTR-Einträgen für jede VCF-Verwaltungs-Appliance und jeden Amazon EVS-Host in Ihrer Bereitstellung erstellen. Weitere Informationen finden Sie unter the section called “DNS-Server konfigurieren”.
- Amazon EVS VLAN-Subnetz-CIDR-Blöcke für jedes VLAN-Subnetz, das Amazon EVS bei der Umgebungserstellung für Sie bereitstellt. CIDR-Blöcke müssen eine Mindestgröße von /28 Netmask und eine Maximalgröße von /24 Netmask haben. CIDR-Blöcke dürfen sich nicht überlappen.
- Eine Amazon VPC Route-Server-Instanz mit aktivierter Route-Server-Propagierung.
- Zwei Route-Server-Endpunkte im Dienstzugriffssubnetz.
- Zwei Route Server-Peers, die die NSX Edge-Knoten, die Amazon EVS mit Route Server-Endpunkten bereitstellt, miteinander verbinden.

Tier-0-Gateway

Das Tier-0-Gateway verarbeitet den gesamten Nord-Süd-Verkehr zwischen den logischen und physischen Netzwerken und wird im NSX-Overlay-Netzwerk erstellt. Dieses Tier-0-Gateway wird als Teil der Amazon EVS-Bereitstellung erstellt.

> **Note**
>
> Amazon EVS unterstützt nur ein Tier-0-Gateway für einen Active/Standby NSX Edge-Cluster mit zwei NSX Edge-Knoten.

Tier-1-Gateway

Das Tier-1-Gateway verarbeitet den Ost-West-Verkehr zwischen gerouteten Netzwerksegmenten innerhalb einer Umgebung und wird im NSX Overlay-Netzwerk erstellt. Das Tier-1-Gateway verfügt über Downlink-Verbindungen zu Segmenten und Uplink-Verbindungen zum Tier-0-Gateway. Sie können bei Bedarf zusätzliche Tier-1-Gateways erstellen und konfigurieren.

NSX Edge-Cluster

Amazon EVS verwendet die NSX Manager-Schnittstelle, um einen NSX Edge-Cluster mit zwei NSX Edge-Knoten bereitzustellen, die im Modus ausgeführt werden. Active/Standby Dieser NSX Edge-Cluster stellt die Plattform bereit, auf der die Tier-0- und Tier-1-Gateways zusammen mit VPN-Verbindungen und deren BGP-Routing-Maschinen ausgeführt werden. IPsec

Amazon EVS-Ressourcen

Amazon EVS stellt bei der Erstellung der Umgebung die folgenden AWS Ressourcen bereit. Diese Ressourcen werden in der VPC angezeigt, auf die Sie Amazon EVS zugreifen dürfen, und sind in der AWS-Managementkonsole und AWS CLI nach ihrer Erstellung sichtbar.

> **Important**
>
> Eine Änderung dieser Ressourcen außerhalb der Amazon EVS-Konsole und API kann sich auf die Verfügbarkeit und Stabilität Ihrer Amazon EVS-Umgebung auswirken.

- Elastische Netzwerkschnittstellen von Amazon EVS, die Konnektivität zu Ihren VCF-Appliances und -Hosts ermöglichen.

- Amazon EVS ESX-Hosts, die auf Amazon EC2 Bare-Metal-Instances ausgeführt werden. Weitere Informationen finden Sie unter the section called “Amazon EVS-Host”.

  > **Important**
  >
  > Ihre Amazon EVS-Umgebung muss mindestens 4 Hosts und nicht mehr als 16 Hosts haben. Amazon EVS unterstützt nur Umgebungen mit 4 bis 16 Hosts.

- Amazon EVS VLAN-Subnetze, die Ihre VPC mit VCF-Appliances verbinden. Weitere Informationen finden Sie unter the section called “Amazon EVS VLAN-Subnetz”.

Amazon Elastic VMware Service einrichten

Um Amazon EVS verwenden zu können, müssen Sie andere AWS Dienste konfigurieren und Ihre Umgebung so einrichten, dass sie die Anforderungen der VMware Cloud Foundation (VCF) erfüllt. Eine zusammenfassende Checkliste der Bereitstellungsvoraussetzungen finden Sie unter. the section called “Checkliste für die Bereitstellung”

Themen

- Melden Sie sich an für AWS
- Erstellen eines IAM-Benutzers
- Erstellen Sie eine IAM-Rolle, um Amazon EVS-Berechtigungen an einen IAM-Benutzer zu delegieren
- Melden Sie sich für einen AWS Business-, AWS Enterprise On-Ramp- oder AWS Enterprise Support-Plan an
- Kontingente überprüfen
- VPC-CIDR-Größen planen
- Erstellen Sie eine VPC mit Subnetzen
- Konfigurieren Sie die VPC-Hauptroutentabelle
- Konfigurieren Sie den DHCP-Optionssatz Ihrer VPC
- Erstellen und konfigurieren Sie die VPC-Route-Server-Infrastruktur
- Erstellen Sie ein Transit-Gateway für lokale Konnektivität
- Erstellen Sie eine Amazon EC2 EC2-Kapazitätsreservierung
- Richten Sie das ein AWS CLI
- Erstellen Sie ein Amazon EC2 key pair
- Bereiten Sie Ihre Umgebung auf VMware Cloud Foundation (VCF) vor
- Erwerben von VCF-Lizenzschlüsseln
- VMware HCX-Voraussetzungen
- Checkliste für die Bereitstellung von Amazon EVS

Melden Sie sich an für AWS

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

1. Öffne https://portal.aws.amazon.com/billing/ die Anmeldung.
2. Folgen Sie den Online-Anweisungen.

Erstellen eines IAM-Benutzers

1. Melden Sie sich als Kontoinhaber bei der IAM-Konsole an, indem Sie Root-Benutzer auswählen und die E-Mail-Adresse Ihres AWS Kontos eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   > **Note**
   >
   > Wir empfehlen nachdrücklich, die bewährten Methoden mit dem `Administrator`-IAM-Benutzer unten zu verwenden und die Anmeldeinformationen des Stammbenutzers an einem sicheren Ort abzulegen. Melden Sie sich als Root-Benutzer an, um einige Konto- und Service-Verwaltungsaufgaben durchzuführen.

2. Wählen Sie im Navigationsbereich Benutzer und dann Benutzer erstellen aus.
3. Geben Sie unter User Name (Benutzername) den Text `Administrator` ein.
4. Aktivieren Sie das Kontrollkästchen neben Zugriff auf die AWS Managementkonsole. Wählen Sie dann Custom password (Benutzerdefiniertes Passwort) aus und geben Sie danach ein neues Passwort in das Textfeld ein.
5. (Optional) Standardmäßig AWS muss der neue Benutzer bei der ersten Anmeldung ein neues Passwort erstellen. Sie können das Kontrollkästchen neben User must create a new password at next sign-in (Benutzer muss bei der nächsten Anmeldung ein neues Passwort erstellen) deaktivieren, damit der neue Benutzer sein Kennwort nach der Anmeldung zurücksetzen kann.
6. Wählen Sie Next: Permissions (Weiter: Berechtigungen) aus.
7. Wählen Sie unter Set permissions (Berechtigungen festlegen) die Option Add user to group (Benutzer der Gruppe hinzufügen) aus.
8. Wählen Sie Create group (Gruppe erstellen) aus.
9. Geben Sie im Dialogfeld Create group (Gruppe erstellen) unter Group name (Gruppenname) den Wert `Administrators` ein.
10. Wählen Sie Richtlinien filtern und anschließend die Funktion für AWS verwaltete Jobs aus, um den Tabelleninhalt zu filtern.

11. Aktivieren Sie in der Richtlinienliste das Kontrollkästchen für AdministratorAccess. Wählen Sie dann Create group (Gruppe erstellen) aus.

> **Note**
>
> Sie müssen den IAM-Benutzer- und Rollenzugriff auf Billing aktivieren, bevor Sie die `AdministratorAccess` Berechtigungen für den Zugriff auf die AWS Billing and Cost Management-Konsole verwenden können. Befolgen Sie hierzu die Anweisungen in Schritt 1 des Tutorials zum Delegieren des Zugriffs auf die Abrechnungskonsole.

12. Kehren Sie zur Gruppenliste zurück und aktivieren Sie das Kontrollkästchen der neuen Gruppe. Möglicherweise müssen Sie Refresh (Aktualisieren) auswählen, damit die Gruppe in der Liste angezeigt wird.
13. Wählen Sie Next: Tags (Weiter: Tags) aus.
14. (Optional) Fügen Sie dem Benutzer Metadaten hinzu, indem Sie Markierungen als Schlüssel-Wert-Paare anfügen. Weitere Informationen zur Verwendung von Markierungen in IAM finden Sie unter Tagging von IAM-Entitäten im IAM-Benutzerhandbuch.
15. Wählen Sie Next: Review (Weiter: Prüfen) aus, damit die Liste der Gruppenmitgliedschaften angezeigt wird, die dem neuen Benutzer hinzugefügt werden soll. Wenn Sie bereit sind, fortzufahren, wählen Sie Create user (Benutzer erstellen) aus.

Sie können dasselbe Verfahren verwenden, um weitere Gruppen und Benutzer zu erstellen und Ihren Benutzern Zugriff auf Ihre AWS Kontoressourcen zu gewähren. Informationen zur Verwendung von Richtlinien, die Benutzerberechtigungen auf bestimmte AWS Ressourcen beschränken, finden Sie unter Zugriffsverwaltung und Beispielrichtlinien.

Erstellen Sie eine IAM-Rolle, um Amazon EVS-Berechtigungen an einen IAM-Benutzer zu delegieren

Sie können Rollen verwenden, um den Zugriff auf Ihre Ressourcen zu delegieren. AWS Mit IAM-Rollen können Sie Vertrauensbeziehungen zwischen Ihrem vertrauenswürdigen Konto und anderen AWS vertrauenswürdigen Konten einrichten. Das vertrauenswürdige Konto besitzt die Ressource, auf die zugegriffen werden soll, und das vertrauenswürdige Konto enthält die Benutzer, die Zugriff auf die Ressource benötigen.

Nachdem Sie die Vertrauensstellung erstellt haben, kann ein IAM-Benutzer oder eine Anwendung aus dem vertrauenswürdigen Konto den `AssumeRole` API-Vorgang AWS -Security-Token-Service (AWS STS) verwenden. Dieser Vorgang stellt temporäre Sicherheitsanmeldedaten bereit, die den Zugriff auf AWS Ressourcen in Ihrem Konto ermöglichen. Weitere Informationen finden Sie im Benutzerhandbuch unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS Identity and Access Management IAM-Benutzer.

Gehen Sie wie folgt vor, um eine IAM-Rolle mit einer Berechtigungsrichtlinie zu erstellen, die den Zugriff auf Amazon EVS-Operationen ermöglicht.

> **Note**
>
> Amazon EVS unterstützt nicht die Verwendung eines Instance-Profils zur Übergabe einer IAM-Rolle an eine EC2-Instance.

Example

IAM console

1. Gehen Sie zur IAM-Konsole.
2. Wählen Sie im linken Menü Richtlinien aus.
3. Wählen Sie Richtlinie erstellen aus.
4. Erstellen Sie im Richtlinien-Editor eine Berechtigungsrichtlinie, die Amazon EVS-Operationen ermöglicht. Eine Beispielrichtlinie finden Sie unter the section called “Erstellen und verwalten Sie eine Amazon EVS-Umgebung”. Alle verfügbaren Amazon EVS-Aktionen, Ressourcen und Bedingungsschlüssel finden Sie unter Aktionen in der Service Authorization Reference.
5. Wählen Sie Weiter aus.
6. Geben Sie unter Richtlinienname einen aussagekräftigen Richtliniennamen ein, um diese Richtlinie zu identifizieren.
7. Überprüfen Sie die in dieser Richtlinie definierten Berechtigungen.
8. (Optional) Fügen Sie Stichwörter hinzu, um diese Ressource leichter identifizieren, organisieren oder nach ihr suchen zu können.
9. Wählen Sie Richtlinie erstellen aus.
10. Wählen Sie im Menü auf der linken Seite Rollen aus.
11. Wählen Sie Rolle erstellen aus.

12. Wählen Sie unter Vertrauenswürdiger Entitätstyp die Option AWS-Konto.
13. Geben Sie unter An das Konto an AWS-Konto , für das Sie Amazon EVS-Aktionen ausführen möchten, und wählen Sie Weiter.
14. Wählen Sie auf der Seite Berechtigungen hinzufügen die Berechtigungsrichtlinie aus, die Sie zuvor erstellt haben, und klicken Sie auf Weiter.
15. Geben Sie unter Rollenname einen aussagekräftigen Namen ein, um diese Rolle zu identifizieren.
16. Überprüfen Sie die Vertrauensrichtlinie und stellen Sie sicher, dass die richtige AWS-Konto Person als Principal aufgeführt ist.
17. (Optional) Fügen Sie Stichwörter hinzu, um diese Ressource leichter identifizieren, organisieren oder nach ihr suchen zu können.
18. Wählen Sie Rolle erstellen aus.

AWS CLI

1. Kopieren Sie den folgenden Inhalt in eine JSON-Datei mit Vertrauensrichtlinien. Ersetzen Sie für den Prinzipal-ARN die AWS-Konto Beispiel-ID und den `service-user` Namen durch Ihre eigene AWS-Konto ID und Ihren eigenen IAM-Benutzernamen.

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

2. Erstellen Sie die Rolle. Ersetzen Sie es durch `evs-environment-role-trust-policy.json` den Namen Ihrer Vertrauensrichtlinien-Datei.

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

3. Erstellen Sie eine Berechtigungsrichtlinie, die Amazon EVS-Operationen ermöglicht, und fügen Sie die Richtlinie der Rolle hinzu. Ersetzen Sie `myAmazonEVSEnvironmentRole` durch den Namen Ihrer Rolle. Eine Beispielrichtlinie finden Sie unter the section called “Erstellen und verwalten Sie eine Amazon EVS-Umgebung”. Alle verfügbaren Amazon EVS-Aktionen, Ressourcen und Bedingungsschlüssel finden Sie unter Aktionen in der Service Authorization Reference.

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

Melden Sie sich für einen AWS Business-, AWS Enterprise On-Ramp- oder AWS Enterprise Support-Plan an

Amazon EVS setzt voraus, dass Kunden für einen AWS Business-, AWS Enterprise On-Ramp- oder AWS Enterprise Support-Plan angemeldet sind, um kontinuierlichen Zugang zu technischem Support und Architekturberatung zu erhalten. AWS Business Support ist die AWS Mindest-Supportstufe, die die Amazon EVS-Anforderungen erfüllt. Wenn Sie geschäftskritische Workloads haben, empfehlen wir, sich für AWS Enterprise On-Ramp- oder Enterprise Support-Pläne zu registrieren. AWS Weitere Informationen finden Sie unter AWS Supportpläne vergleichen.

> **Important**
>
> Die Erstellung der Amazon EVS-Umgebung schlägt fehl, wenn Sie sich nicht für einen AWS Business-, AWS Enterprise On-Ramp- oder AWS Enterprise Support-Plan anmelden.

Kontingente überprüfen

Um die Erstellung einer Amazon EVS-Umgebung zu ermöglichen, stellen Sie sicher, dass Ihr Konto über die erforderlichen Mindestkontingente auf Kontoebene verfügt. Weitere Informationen finden Sie unter Servicekontingente.

> **Important**
>
> Die Erstellung der Amazon EVS-Umgebung schlägt fehl, wenn der Quotenwert für die Hostanzahl pro EVS-Umgebung nicht mindestens 4 beträgt.

VPC-CIDR-Größen planen

Wenn Sie eine Amazon EVS-Umgebung erstellen, müssen Sie einen VPC-CIDR-Block angeben. Der VPC-CIDR-Block kann nach der Erstellung der Umgebung nicht mehr geändert werden und es muss genügend Speicherplatz reserviert sein, um die erforderlichen EVS-Subnetze und Hosts aufzunehmen, die Amazon EVS während der Bereitstellung der Umgebung erstellt. Daher ist es wichtig, die CIDR-Blockgröße sorgfältig zu planen und dabei die Amazon EVS-Anforderungen und Ihre future Skalierungsanforderungen vor der Bereitstellung zu berücksichtigen. Amazon EVS benötigt einen VPC-CIDR-Block mit einer Mindestgröße von /22-Netzmaske, um ausreichend Speicherplatz für die erforderlichen EVS-Subnetze und Hosts bereitzustellen. Weitere Informationen finden Sie unter the section called “Überlegungen zum Amazon EVS-Netzwerk”.

> **Important**
>
> Stellen Sie sicher, dass Sie über ausreichend IP-Adressraum sowohl für Ihr VPC-Subnetz als auch für die VLAN-Subnetze verfügen, die Amazon EVS für VCF-Appliances erstellt. Der VPC-CIDR-Block muss eine Mindestgröße von /22-Netzmaske haben, um ausreichend Speicherplatz für die erforderlichen EVS-Subnetze und Hosts bereitzustellen.

> **Note**
>
> Amazon EVS unterstützt IPv6 derzeit nicht.

Erstellen Sie eine VPC mit Subnetzen

Amazon EVS stellt Ihre Umgebung in einer von Ihnen bereitgestellten VPC bereit. Diese VPC muss ein Subnetz für den Zugriff auf den Amazon EVS-Service () enthalten. the section called “Subnetz für den Servicezugriff” Schritte zum Erstellen einer VPC mit Subnetzen für Amazon EVS finden Sie unter. the section called “Erstellen Sie eine VPC mit Subnetzen und Routentabellen”

Konfigurieren Sie die VPC-Hauptroutentabelle

Amazon EVS-VLAN-Subnetze sind implizit der VPC-Hauptroutentabelle zugeordnet. Um die Konnektivität zu abhängigen Diensten wie DNS oder lokalen Systemen für eine erfolgreiche Implementierung der Umgebung zu aktivieren, müssen Sie die Haupt-Routing-Tabelle so konfigurieren, dass Datenverkehr zu diesen Systemen zugelassen wird. Weitere Informationen finden Sie unter the section called “Ordnen Sie Amazon EVS-VLAN-Subnetze explizit einer VPC-Routentabelle zu”.

> **Important**
>
> Amazon EVS unterstützt die Verwendung einer benutzerdefinierten Routentabelle erst, nachdem die Amazon EVS-Umgebung erstellt wurde. Benutzerdefinierte Routing-Tabellen sollten bei der Erstellung der Amazon EVS-Umgebung nicht verwendet werden, da dies zu Verbindungsproblemen führen kann.

Anforderungen an die Gateway-Route

Konfigurieren Sie Routen für diese Gateway-Typen auf der Grundlage Ihrer Konnektivitätsanforderungen:

- NAT-Gateway (NGW)
  - Optional für Internetzugang nur für ausgehende Verbindungen.
  - Muss sich in einem öffentlichen Subnetz mit Internet-Gateway-Zugang befinden.
  - Fügen Sie dem NAT-Gateway Routen von privaten Subnetzen und EVS-VLAN-Subnetzen hinzu.
  - Weitere Informationen finden Sie unter Arbeiten mit NAT-Gateways im Amazon VPC-Benutzerhandbuch.
- Transit-Gateway (TGW)
  - Erforderlich für lokale Konnektivität über AWS Direct Connect und AWS Site-to-Site VPN.
  - Fügen Sie Routen für lokale Netzwerkbereiche hinzu.
  - Konfigurieren Sie die Routenverbreitung, wenn Sie BGP verwenden.
  - Weitere Informationen finden Sie unter Transit-Gateways in Amazon VPC Transit Gateways im Amazon VPC-Benutzerhandbuch.

Best Practices

- Dokumentieren Sie alle Routentabellenkonfigurationen.
- Verwenden Sie konsistente Benennungskonventionen.
- Prüfen Sie regelmäßig Ihre Routing-Tabellen.
- Testen Sie die Konnektivität, nachdem Sie Änderungen vorgenommen haben.
- Sichern Sie die Routentabellenkonfigurationen.
- Überwachen Sie den Zustand und die Ausbreitung der Route.

Weitere Informationen zur Arbeit mit Routentabellen finden Sie unter Route-Tabellen konfigurieren im Amazon VPC-Benutzerhandbuch.

Konfigurieren Sie den DHCP-Optionssatz Ihrer VPC

Important

Ihre Umgebungsbereitstellung schlägt fehl, wenn Sie die folgenden Amazon EVS-Anforderungen nicht erfüllen:

- Nehmen Sie eine primäre DNS-Server-IP-Adresse und eine sekundäre DNS-Server-IP-Adresse in den DHCP-Optionssatz auf.
- Fügen Sie eine DNS-Forward-Lookupzone mit A-Einträgen für jede VCF-Verwaltungs-Appliance und jeden Amazon EVS-Host in Ihre Bereitstellung ein.
- Fügen Sie eine DNS-Reverse-Lookupzone mit PTR-Einträgen für jede VCF-Verwaltungs-Appliance und jeden Amazon EVS-Host in Ihre Bereitstellung ein.
- Konfigurieren Sie die Haupt-Routing-Tabelle der VPC, um sicherzustellen, dass eine Route zu Ihren DNS-Servern vorhanden ist.
- Stellen Sie sicher, dass Ihre Domainnamenregistrierung gültig und nicht abgelaufen ist, und dass keine doppelten Hostnamen oder IP-Adressen vorhanden sind.
- Konfigurieren Sie Ihre Sicherheitsgruppen und Netzwerk-Zugriffskontrolllisten (ACLs), damit Amazon EVS kommunizieren kann mit:
  - DNS-Server über TCP/UDP Port 53.
  - Host-Management-VLAN-Subnetz über HTTPS und SSH.

- Verwaltungs-VLAN-Subnetz über HTTPS und SSH.

Weitere Informationen finden Sie unter the section called “Konfigurieren von DNS- und NTP-Servern mithilfe des VPC-DHCP-Optionssatzes”.

Erstellen und konfigurieren Sie die VPC-Route-Server-Infrastruktur

Amazon EVS verwendet Amazon VPC Route Server, um BGP-basiertes dynamisches Routing zu Ihrem VPC-Underlay-Netzwerk zu ermöglichen. Sie müssen einen Routenserver angeben, der Routen mit mindestens zwei Route-Server-Endpunkten im Service-Access-Subnetz teilt. Die auf den Route-Server-Peers konfigurierten Peer-ASNs müssen übereinstimmen und die Peer-IP-Adressen müssen eindeutig sein.

Important

Ihre Umgebungsbereitstellung schlägt fehl, wenn Sie die folgenden Amazon EVS-Anforderungen für die VPC-Route-Server-Konfiguration nicht erfüllen:

- Sie müssen mindestens zwei Route-Server-Endpunkte im Service-Access-Subnetz konfigurieren.
- Bei der Konfiguration des Border Gateway Protocol (BGP) für das Tier-0-Gateway muss der Peer-ASN-Wert des VPC-Routenservers mit dem NSX Edge-Peer-ASN-Wert übereinstimmen.
- Bei der Erstellung der beiden Route-Server-Peers müssen Sie für jeden Endpunkt eine eindeutige IP-Adresse aus dem NSX-Uplink-VLAN verwenden. Diese beiden IP-Adressen werden den NSX Edges während der Bereitstellung der Amazon EVS-Umgebung zugewiesen.
- Wenn Sie die Route-Server-Propagierung aktivieren, müssen Sie sicherstellen, dass alle Routing-Tabellen, die weitergegeben werden, mindestens eine explizite Subnetzzuweisung haben. BGP-Routenankündigung schlägt fehl, wenn weitergegebene Routentabellen keine explizite Subnetzzuweisung haben.

> **Note**
>
> Für die Erkennung der Route-Server-Peer-Verfügbarkeit unterstützt Amazon EVS nur den standardmäßigen BGP-Keepalive-Mechanismus. Amazon EVS unterstützt keine bidirektionale Multi-Hop-Weiterleitungserkennung (BFD).

Voraussetzungen

Bevor Sie anfangen, benötigen Sie:

- Ein VPC-Subnetz für Ihren Routenserver.
- IAM-Berechtigungen zur Verwaltung von VPC-Routenserver-Ressourcen.
- Ein BGP-ASN-Wert für den Routenserver (Amazon-seitige ASN). Der Wert muss im Bereich von 1-4294967295 liegen.
- Eine Peer-ASN für Ihren Routenserver als Peer mit dem NSX Tier-0-Gateway. Die im Routenserver und im NSX Tier-0-Gateway eingegebenen Peer-ASN-Werte müssen übereinstimmen. Die Standard-ASN für eine NSX Edge-Appliance ist 65000.

Schritte

Schritte zum Einrichten des VPC-Routenservers finden Sie im Tutorial Erste Schritte für Route Server.

> **Note**
>
> Wenn Sie ein NAT-Gateway oder ein Transit-Gateway verwenden, stellen Sie sicher, dass Ihr Routenserver korrekt konfiguriert ist, um NSX-Routen an die VPC-Routentabelle (n) weiterzuleiten.

> **Note**
>
> Wir empfehlen, persistente Routen für die Route-Server-Instanz mit einer dauerhaften Dauer zwischen 1 und 5 Minuten zu aktivieren. Wenn diese Option aktiviert ist, werden Routen

in der Routingdatenbank des Routenservers beibehalten, auch wenn alle BGP-Sitzungen enden.

> **Note**
>
> Der BGP-Konnektivitätsstatus ist inaktiv, bis die Amazon EVS-Umgebung bereitgestellt und betriebsbereit ist.

Erstellen Sie ein Transit-Gateway für lokale Konnektivität

Sie können die Konnektivität zwischen Ihrem lokalen Rechenzentrum und Ihrer AWS Infrastruktur mithilfe eines zugehörigen Transit-Gateways oder Direct Connect mithilfe eines AWS Site-to-Site VPN-Anhangs zu einem Transit-Gateway konfigurieren. Weitere Informationen finden Sie unter the section called “Konfigurieren Sie die lokale Netzwerkkonnektivität (optional)”.

Erstellen Sie eine Amazon EC2 EC2-Kapazitätsreservierung

Amazon EVS startet Amazon EC2-Metal-Instances, die die ESX-Hosts in Ihrer Amazon EVS-Umgebung sind. Um sicherzustellen, dass Ihnen beim Hinzufügen von Hosts genügend Kapazität zur Verfügung steht, empfehlen wir Ihnen, eine Amazon EC2 EC2-Kapazitätsreservierung zu beantragen. Sie können jederzeit eine Kapazitätsreservierung erstellen und wählen, wann sie beginnt. Sie können eine Kapazitätsreservierung zur sofortigen Nutzung oder eine Kapazitätsreservierung für einen future Termin beantragen. Weitere Informationen finden Sie unter Reservieren von Rechenkapazität mit EC2-On-Demand-Kapazitätsreservierungen im Amazon Elastic Compute Cloud-Benutzerhandbuch.

Richten Sie das ein AWS CLI

Das AWS CLI ist ein Befehlszeilentool für die Arbeit AWS-Services, einschließlich Amazon EVS. Es wird auch verwendet, um IAM-Benutzer oder -Rollen für den Zugriff auf die Amazon EVS-Virtualisierungsumgebung und andere AWS Ressourcen von Ihrem lokalen Computer aus zu authentifizieren. Um AWS Ressourcen über die Befehlszeile bereitzustellen, benötigen Sie eine AWS Zugriffsschlüssel-ID und einen geheimen Schlüssel, die Sie in der Befehlszeile verwenden können. Anschließend müssen diese Anmeldeinformationen in der AWS CLI konfiguriert werden. Weitere Informationen finden Sie AWS CLI im AWS Command Line Interface Benutzerhandbuch für Version 2.

Erstellen Sie ein Amazon EC2 key pair

Amazon EVS verwendet ein Amazon EC2 key pair, das Sie bei der Erstellung der Umgebung angeben, um eine Verbindung zu Ihren Hosts herzustellen. Um ein key pair zu erstellen, folgen Sie den Schritten unter key pair für Ihre Amazon EC2 Instance erstellen im Amazon Elastic Compute Cloud Benutzerhandbuch.

Bereiten Sie Ihre Umgebung auf VMware Cloud Foundation (VCF) vor

Bevor Sie Ihre Amazon EVS-Umgebung bereitstellen, muss Ihre Umgebung die Infrastrukturanforderungen der VMware Cloud Foundation (VCF) erfüllen. Ausführliche VCF-Voraussetzungen finden Sie in der Arbeitsmappe zur Planung und Vorbereitung in der VMware Cloud Foundation-Produktdokumentation.

Sie sollten sich auch mit den Anforderungen von VCF 5.2.x vertraut machen. In den Versionshinweisen zu VCF 5.2.x finden Sie relevante Versionsinformationen.

> **Note**
>
> Informationen zu den von Amazon EVS bereitgestellten VCF-Versionen finden Sie unter. the section called “VCF-Versionen und EC2-Instances”

Erwerben von VCF-Lizenzschlüsseln

Um Amazon EVS verwenden zu können, müssen Sie einen VCF-Lösungsschlüssel und einen vSAN-Lizenzschlüssel angeben. Die spezifischen Anforderungen an die Anzahl der Kerne und die vSAN-Kapazität hängen vom ausgewählten Instanztyp ab. Einzelheiten zu den Mindestschwellenwerten für Kern und Kapazität für Ihren Instance-Typ finden Sie unter the section called “VCF-Abonnements” Konfiguration. Weitere Informationen zu VCF-Lizenzen finden Sie unter Verwaltung von Lizenzschlüsseln in VMware Cloud Foundation im Cloud VMware Foundation-Administrationshandbuch.

> **Important**
>
> Verwenden Sie die SDDC Manager-Benutzeroberfläche, um die VCF-Lösung und die vSAN-Lizenzschlüssel zu verwalten. Amazon EVS erfordert, dass Sie gültige VCF-Lösungs- und

vSAN-Lizenzschlüssel im SDDC Manager verwalten, damit der Service ordnungsgemäß funktioniert.

> **Note**
>
> Ihre VCF-Lizenz steht Amazon EVS in allen AWS Regionen zur Verfügung, um die Einhaltung der Lizenzbestimmungen zu gewährleisten. Amazon EVS validiert keine Lizenzschlüssel. Besuchen Sie den Broadcom-Support, um Lizenzschlüssel zu validieren.

VMware HCX-Voraussetzungen

Sie können VMware HCX verwenden, um Ihre vorhandenen VMware basierten Workloads zu Amazon EVS zu migrieren. Bevor Sie VMware HCX mit Amazon EVS verwenden, stellen Sie sicher, dass die folgenden erforderlichen Aufgaben abgeschlossen wurden.

> **Note**
>
> VMware HCX ist standardmäßig nicht in der EVS-Umgebung installiert.

- Bevor Sie VMware HCX mit Amazon EVS verwenden können, müssen die Mindestanforderungen an die Netzwerkunterlage erfüllt sein. Weitere Informationen finden Sie unter Mindestanforderungen für Network Underlay im VMware HCX-Benutzerhandbuch.
- Vergewissern Sie sich, dass VMware NSX in der Umgebung installiert und konfiguriert ist. Weitere Informationen finden Sie im VMware NSX-Installationshandbuch.
- Stellen Sie sicher, dass VMware HCX aktiviert und in der Umgebung installiert ist. Weitere Informationen zur Aktivierung und Installation von VMware HCX finden Sie unter About Getting Started with VMware HCX im Handbuch Erste Schritte mit VMware HCX.
- Wenn Sie eine HCX-Internetverbindung benötigen, müssen Sie die folgenden erforderlichen Aufgaben ausführen:
  - Stellen Sie sicher, dass Ihr IPAM-Kontingent für von Amazon bereitgestellte zusammenhängende öffentliche IPv4 CIDR-Block-Netzmaskenlänge /28 oder höher ist.

> **Important**
>
> Für HCX-Internetkonnektivität erfordert Amazon EVS die Verwendung eines IPv4 CIDR-Blocks aus einem öffentlichen IPAM-Pool mit einer Netzmaskenlänge von /28 oder mehr. Die Verwendung eines beliebigen CIDR-Blocks mit einer Netzmaskenlänge von weniger als /28 führt zu HCX-Konnektivitätsproblemen. Weitere Informationen zur Erhöhung der IPAM-Kontingente finden Sie unter Kontingente für Ihr IPAM.

- Erstellen Sie einen IPAM und einen öffentlichen IPv4 IPAM-Pool mit CIDR, die eine Netzmasken-Mindestlänge von /28 haben.
- Weisen Sie den HCX Manager- und HCX Interconnect (HCX-IXEIPs) -Appliances mindestens zwei Elastic IP-Adressen () aus dem IPAM-Pool zu. Weisen Sie jeder HCX-Netzwerk-Appliance, die Sie bereitstellen müssen, eine zusätzliche Elastic IP-Adresse zu.
- Fügen Sie den öffentlichen IPv4 CIDR-Block als zusätzlichen CIDR zu Ihrer VPC hinzu.

Weitere Informationen zum HCX-Setup finden Sie unter und. the section called “Wählen Sie Ihre HCX-Konnektivitätsoption” the section called “HCX-Konnektivitätsoptionen”

Checkliste für die Bereitstellung von Amazon EVS

Dieser Abschnitt enthält eine Liste der Voraussetzungen, die erfüllt sein müssen, um eine erfolgreiche Bereitstellung der Amazon EVS-Umgebung zu ermöglichen.

Informationen zum VCF-Lizenzschlüssel

Komponente	Description	Mindestanforderungen	Beispielwert (e)
Seiten-ID	Von Broadcom bereitgestellte Site-ID für den Zugriff auf das Broadcom-Supportportal.	In der Anfrage zur Erstellung der EVS-Umgebung muss eine Site-ID von Broadcom angegeben werden.	01234567
VCF-Lösungsschlüssel	Ein einziger VCF-Lizenzschlüssel, der Funktionen des	In der Anfrage zur Erstellung der EVS-Umgebung muss ein	ABCDE-FGHIJ-KLMNO-PQRSTU-VWXYZ

Komponente	Description	Mindestanforderungen	Beispielwert (e)
	gesamten VCF-Stacks freischaltet, einschließlich vSphere, NSX, SDDC Manager und vCenter Server.	gültiger aktiver VCF-Lösungsschlüssel angegeben werden. Der Schlüssel darf nicht bereits von einer vorhandenen EVS-Umgebung verwendet werden.	
vSAN-Lizenzschlüssel	Mit einem vSAN-Lizenzschlüssel können Sie die vSAN-Software in einer VCF-Umgebung aktivieren und verwenden.	In der Anfrage zur Erstellung der EVS-Umgebung muss ein gültiger aktiver vSAN-Lizenzschlüssel angegeben werden. Der Schlüssel darf nicht bereits von einer vorhandenen EVS-Umgebung verwendet werden.	ABCDE-FGHIJ-KLMNO-PQRSTU-VWXYZ

AWS Konto- und Regionsinformationen

Komponente	Description	Mindestanforderungen	Beispielwert (e)
AWS Konto-ID-Nummer	Mit dem AWS Konto können Sie AWS Ressourcen erstellen und verwalten und auf AWS Dienste zugreifen.	Muss Zugriff auf ein AWS Konto haben.	999999999999

Komponente	Description	Mindestanforderungen	Beispielwert (e)
AWS Region	Ein physisches geografisches Gebiet, in dem mehrere isolierte Rechenzentren, sogenannte Availability Zones, AWS verwaltet werden.	Sie müssen eine AWS Region angeben, in der Amazon EVS bereitgestellt werden soll. Eine Liste der Regionen, in denen Amazon EVS derzeit verfügbar ist, finden Sie unter Amazon Elastic VMware Service Endpoints and Quotas im AWS General Reference Guide.	USA West (Oregon)

AWS Transit Gateway für lokale Rechenzentrumskonnektivität

Komponente	Description	Mindestanforderungen	Beispielwert (e)
Transit-Gateway-ID	Ein Transit-Gateway fungiert als regionaler virtueller Router für den Datenverkehr zwischen Ihrer VPC und lokalen Netzwerken.	Sie müssen ein Transit-Gateway verwenden, um eine Amazon EVS-Umgebung mit Ihren lokalen Netzwerken zu verbinden.	Beispiel für TGW-0262A0E521
Konnektivitätsmethode	Um Ihre lokalen Netzwerke mit einer Amazon EVS-Umgebung zu verbinden, müssen Sie ein Transit-Gateway mit	Entscheiden Sie, ob Sie AWS Direct Connect, AWS Site-to-Site VPN oder eine Kombination aus beidem verwenden	AWS Site-to-Site VPN mit AWS Direktverbindung

Komponente	Description	Mindestanforderungen	Beispielwert (e)
	AWS Direct Connect oder AWS Site-to-Site VPN verwenden.	möchten. Weitere Informationen zur Verwendung von Site-to-Site VPN mit Direct Connect finden Sie unter Privates AWS Site-to-Site IP-VPN mit AWS Direct Connect.	

VPC für Amazon EVS-Umgebung

Komponente	Description	Mindestanforderungen	Beispielwert (e)
VPC-ID	Eine VPC ist ein virtuelles Netzwerk, das einem herkömmlichen Netzwerk sehr ähnlich ist, das Sie in Ihrem eigenen Rechenzentrum betreiben würden.	Jede Amazon VPC kann für die Bereitstellung der Umgebung verwendet werden.	vpc-0abcdef1234567890
VPC-CIDR-Block	In Amazon VPC definiert ein CIDR-Block den Bereich der IP-Adressen, die in Ihrer VPC verfügbar sind.	Ein CIDR-Block nach RFC 1918 mit einer Mindestgröße von /22-Netzmaske. Der VPC-CIDR-Block muss entsprechend dimensioniert sein, um alle EVS-Subnetze und -Hosts aufzunehm	10.1.0.0/20

Komponente	Description	Mindestanforderungen	Beispielwert (e)
		en, die in Ihrer VPC bereitgestellt werden sollen. Dieser CIDR-Block sollte in Ihren Umgebungen einzigartig sein.	

VPC-Subnetze für die EVS-Umgebung

Komponente	Description	Mindestanforderungen	Beispielwert (e)
Subnetz-ID für den Zugriff auf den Dienst	Ein Service-Access-Subnetz ist ein Standard-VPC-Subnetz, das den Amazon EVS-Servicezugriff ermöglicht. Weitere Informationen finden Sie unter the section called “Subnetz für den Servicezugriff”.	Jedes VPC-Subnetz kann verwendet werden, sofern das Subnetz innerhalb der VPC eine angemessene Größe hat. Wir empfehlen, einen VPC-Subnetz-CIDR-Block mit einer Netzmaske von /24 anzugeben.	subnet-abcdef1234567890e
Dienstzugriff, Subnetz (CIDR)	Ein VPC-Subnetz-CIDR-Block ist ein mithilfe der CIDR-Notation definierter Bereich von IP-Adressen, der einem bestimmten Subnetz innerhalb einer VPC zugewiesen ist.	Das Servicezugriffssubnetz muss entsprechend dimensioniert sein, damit es auch die anderen EVS-Subnetze und Hosts aufnehmen kann, die in Ihrer VPC bereitgestellt werden	10.1.0.0/24

Komponente	Description	Mindestanforderungen	Beispielwert (e)
		sollen. Wir empfehlen, einen VPC-Subnetz-CIDR-Block mit einer Netzmaske von /24 anzugeben.	
AWS ID der Verfügbarkeitszone innerhalb der Region	Ein bestimmter Standort innerhalb einer AWS Region, der so konzipiert ist AZs, dass er vor Ausfällen in anderen Regionen isoliert ist und aus einem oder mehreren Rechenzentren besteht.	Sie können die Availability Zone angeben, in der VPC-Subnetze während der Subnetzerstellung bereitgestellt werden. Weitere Informationen finden Sie unter Erstellen eines Subnetzes im Amazon VPC-Benutzerhandbuch.	us-west-2a

EVS-VLAN-Subnetze für die EVS-Umgebung

Komponente	Description	Mindestanforderungen	Beispielwert (e)
Hostverwaltung VLAN CIDR	Der CIDR-Block für das Host-Management-VLAN-Subnetz. Weitere Informationen finden Sie unter the section called “Hostverwaltung, VLAN-Subnetz”.	Muss eine Mindestgröße von /28 Netmask und eine Maximalgröße von /24 Netmask haben. Darf sich nicht mit einem vorhandenen CIDR-Block überschneiden, der der VPC zugeordnet ist.	10.1.1.0/24

Komponente	Description	Mindestanforderungen	Beispielwert (e)
vMotion VLAN CIDR	Der CIDR-Block für das vMotion-VLAN-Subnetz. Weitere Informationen finden Sie unter the section called “vMotion-VLAN-Subnetz”.	Muss dieselbe Größe wie das Host-Management-VLAN haben.	10.1.2.0/24
vSAN VLAN CIDR	Der CIDR-Block für das vSAN-VLAN-Subnetz. Weitere Informationen finden Sie unter the section called “vSAN-VLAN-Subnetz”.	Muss dieselbe Größe wie das Host-Management-VLAN haben.	10.1.3.0/24
VTEP CLAN APFELWEIN	Der CIDR-Block für das VTEP-VLAN-Subnetz. Weitere Informationen finden Sie unter the section called “VTEP-VLAN-Subnetz”.	Muss dieselbe Größe wie das Host-Management-VLAN haben.	10.1.4.0/24
Edge VTEP VLAN CIDR	Der CIDR-Block für das Edge-VTEP-VLAN-Subnetz. Weitere Informationen finden Sie unter the section called “Edge-VTEP-VLAN-Subnetz”.	Muss eine Mindestgröße von /28 Netmask und eine Maximalgröße von /24 Netmask haben. Darf sich nicht mit einem vorhandenen CIDR-Block überschneiden, der der VPC zugeordnet ist.	10.1.5.0/24

Komponente	Description	Mindestanforderungen	Beispielwert (e)
Verwaltung: VM, VLAN, CIDR	Der CIDR-Block für das VLAN-Subnetz der Management-VM. Weitere Informationen finden Sie unter the section called “VLAN-Subnetz der Verwaltungs-VM”.	Muss eine Mindestgröße von /28 Netmask und eine Maximalgröße von /24 Netmask haben. Darf sich nicht mit einem vorhandenen CIDR-Block überschneiden, der der VPC zugeordnet ist.	10.1.6.0/24
HCX-Uplink-VLAN CIDR	Der CIDR-Block für das HCX-Uplink-VLAN-Subnetz. Weitere Informationen finden Sie unter the section called “HCX-Uplink-VLAN-Subnetz”.	Muss eine Mindestgröße von /28 Netmask und eine Maximalgröße von /24 Netmask haben. Darf sich nicht mit einem vorhandenen CIDR-Block überschneiden, der der VPC zugeordnet ist.	10.1.7.0/24
NSX-Uplink-VLAN CIDR	Der CIDR-Block für das NSX-Uplink-VLAN-Subnetz. Weitere Informationen finden Sie unter the section called “NSX-Uplink-VLAN-Subnetz”.	Muss eine Mindestgröße von /28 Netmask und eine Maximalgröße von /24 Netmask haben. Darf sich nicht mit einem vorhandenen CIDR-Block überschneiden, der der VPC zugeordnet ist.	10.1.8.0/24

Komponente	Description	Mindestanforderungen	Beispielwert (e)
Erweiterung VLAN 1 CIDR	CIDR-Block für das Erweiterungs-VLAN-Subnetz. Weitere Informationen finden Sie unter the section called “Erweiterung: VLAN-Subnetz”.	Muss eine Mindestgröße von /28 Netmask und eine Maximalgröße von /24 Netmask haben. Darf sich nicht mit einem vorhanden en CIDR-Block überschneiden, der der VPC zugeordnet ist.	10.1.9.0/24
Erweiterung VLAN 2 CIDR	CIDR-Block für das Erweiterungs-VLAN-Subnetz. Weitere Informationen finden Sie unter the section called “Erweiterung: VLAN-Subnetz”.	Muss eine Mindestgröße von /28 Netmask und eine Maximalgröße von /24 Netmask haben. Darf sich nicht mit einem vorhanden en CIDR-Block überschneiden, der der VPC zugeordnet ist.	10.1.10.0/24

DNS- und NTP-Infrastruktur

Komponente	Description	Mindestanforderungen	Beispielwert (e)
IP-Adresse des primären DNS-Servers	Der Hauptserver für das Domain Name System (DNS), der als Informationsquelle für alle DNS-Einträge der	Sie können jede gültige, unbenutzte IPv4 Adresse innerhalb des nutzbaren Hostbereichs verwenden.	10.1.1.10

Komponente	Description	Mindestanforderungen	Beispielwert (e)
	Domain verwendet wird.		
IP-Adresse des sekundären DNS-Servers	Ein Backup-DNS-Server für die DNS-Einträge der Domain.	Sie können jede gültige, unbenutzte IPv4 Adresse innerhalb des nutzbaren Hostbereichs verwenden.	10.1.5.25
IP-Adresse des NTP-Servers	Ein NTP-Server (Network Time Protocol) ist ein Gerät oder eine Anwendung, die Uhren innerhalb eines Netzwerks mithilfe des NTP-Standards synchronisiert.	Sie können den standardmäßigen Amazon Time Sync Service mit der lokalen `169.254.169.123` IP-Adresse oder einer anderen NTP-Server-IP-Adresse verwenden.	169.254.169.123 (Amazon Time Sync-Dienst)
FQDN für die VCF-Bereitstellung	Ein vollqualifizierter Domänenname (FQDN) ist der absolute Name eines Geräts in einem Netzwerk. Ein FQDN besteht aus einem Hostnamen und einem Domainnamen.	Ein FQDN kann nur alphanumerische Zeichen, das Minuszeichen (-) und Punkte enthalten, die als Trennzeichen zwischen Bezeichnungen verwendet werden. Muss ein eindeutiger FQDN sein, der gültig und noch nicht abgelaufen ist.	evs.local

VPC-DHCP-Optionssatz

Komponente	Description	Mindestanforderungen	Beispielwert (e)
ID des DHCP-Optionssatzes	Ein DHCP-Optionssatz ist eine Gruppe von Netzwerkeinstellungen, die von Ressourcen in Ihrer VPC, z. B. EC2 Instances, für die Kommunikation über Ihr virtuelles Netzwerk verwendet werden.	Muss mindestens 2 DNS-Server enthalten. Sie können Route 53 oder benutzerdefinierte DNS-Server verwenden. Muss auch Ihren DNS-Domainnamen und einen NTP-Server enthalten.	dopt-0a1b2c3d

EC2 key pair

Komponente	Description	Mindestanforderungen	Beispielwert (e)
EC2 Name key pair	Ein EC2 key pair ist ein Satz von Sicherheitsanmeldedaten, die verwendet werden, um eine sichere Verbindung zu einer EC2 Amazon-Instance herzustellen.	Der Name des Schlüsselpaars muss eindeutig sein.	`my-ec2-key-pair`

VPC-Routing-Tabellen

Komponente	Description	Mindestanforderungen	Beispielwert (e)
ID der Hauptroutentabelle	In Amazon VPC ist die Haupt-Routing-Tabelle die Standard-Routing-Tabelle, die automatisch mit der VPC erstellt wird. Sie regelt den Verkehr für alle VPC-Subnetze, die nicht explizit mit einer anderen Routing-Tabelle verknüpft sind. EVS-VLAN-Subnetze werden implizit der Haupt-Routing-Tabelle Ihrer VPC zugeordnet, wenn Amazon EVS sie erstellt.	Muss so konfiguriert werden, dass Konnektivität zu abhängigen Diensten wie DNS oder lokalen Systemen ermöglicht wird, damit die Umgebung erfolgreich bereitgestellt werden kann.	rtb-0123456789abcdef0

Netzwerk-Zugriffskontrolllisten (ACL)

Komponente	Description	Mindestanforderungen	Beispielwert (e)
Netzwerk-ACL-ID	Eine Network Access Control List (ACL) erlaubt oder verweigert eingehenden oder ausgehenden Datenverkehr auf Subnetzebene.	Muss Amazon EVS die Kommunikation ermöglichen mit: • DNS-Server über TCP/UDP Port 53.	acl-0f62c640e793a38a3

Komponente	Description	Mindestanforderungen	Beispielwert (e)
		• Host-Management-VLAN-Subnetz über HTTPS und SSH. • VLAN-Subnetz der Verwaltungs-VM über HTTPS und SSH.	

DNS-Einträge für VCF-Komponenten

Komponente	Description	Mindestanforderungen	Beispiel für eine IP-Adresse	Beispiel für einen Hostnamen
ESX-Host 1	IP-Adresse und Hostname, die im A-Datensatz und im PTR-Datensatz für ESX-Host 1 definiert sind.	Amazon EVS benötigt eine DNS-Forward-Lookupzone mit A-Einträgen und eine Reverse-Lookupzone mit PTR-Einträgen, die für jeden ESX-Host in jeder EVS-Bereitstellung erstellt wurden.	10.1.0.10	esxi01
ESX-Host 2	IP-Adresse und Hostname, die im A-Datensatz und im PTR-Datensatz für ESX-Host 2 definiert sind.	Amazon EVS benötigt eine DNS-Forward-Lookupzone mit A-Einträgen und eine Reverse-Lookupzone mit	10.1.0.11	esxi02

Komponente	Description	Mindestanforderungen	Beispiel für eine IP-Adresse	Beispiel für einen Hostnamen
		PTR-Einträgen, die für jeden ESX-Host in jeder EVS-Bereitstellung erstellt wurden.		
ESX-Host 3	IP-Adresse und Hostname, die im A-Datensatz und im PTR-Datensatz für ESX-Host 3 definiert sind.	Amazon EVS benötigt eine DNS-Forward-Lookupzone mit A-Einträgen und eine Reverse-Lookupzone mit PTR-Einträgen, die für jeden ESX-Host in jeder EVS-Bereitstellung erstellt wurden.	10.1.0.12	esxi03
ESX-Host 4	IP-Adresse und Hostname, die im A-Datensatz und im PTR-Datensatz für ESX-Host 4 definiert sind.	Amazon EVS benötigt eine DNS-Forward-Lookupzone mit A-Einträgen und eine Reverse-Lookupzone mit PTR-Einträgen, die für jeden ESX-Host in jeder EVS-Bereitstellung erstellt wurden.	10.1.0.13	esxi04

Komponente	Description	Mindestanforderungen	Beispiel für eine IP-Adresse	Beispiel für einen Hostnamen
vCenter Server-Appliance	IP-Adresse und Hostname, die im A-Datensatz und im PTR-Datensatz für die vCenter Server Appliance definiert sind.	Amazon EVS benötigt eine DNS-Forward-Lookupzone mit A-Einträgen und eine Reverse-Lookupzone mit PTR-Einträgen, die für jede VCF-Verwaltungs-Appliance in jeder EVS-Bereitstellung erstellt wurden.	10.1.5.10	vc01
NSX Manager-Cluster	IP-Adresse und Hostname, die im A-Eintrag und im PTR-Datensatz für den NSX Manager-Cluster definiert sind.	Amazon EVS benötigt eine DNS-Forward-Lookupzone mit A-Einträgen und eine Reverse-Lookupzone mit PTR-Einträgen, die für jede VCF-Verwaltungs-Appliance in jeder EVS-Bereitstellung erstellt wurden.	10.1.5.11	nsx

Komponente	Description	Mindestanforderungen	Beispiel für eine IP-Adresse	Beispiel für einen Hostnamen
SDDC Manager-Appliance	IP-Adresse und Hostname, die im A-Datensatz und im PTR-Datensatz für die SDDC Manager-Appliance definiert sind.	Amazon EVS benötigt eine DNS-Forward-Lookupzone mit A-Einträgen und eine Reverse-Lookupzone mit PTR-Einträgen, die für jede VCF-Verwaltungs-Appliance in jeder EVS-Bereitstellung erstellt wurden.	10.1.5.12	sddcm01
Cloud Builder-Appliance	IP-Adresse und Hostname, die im A-Datensatz und im PTR-Datensatz für die Cloud Builder-Appliance definiert sind.	Amazon EVS benötigt eine DNS-Forward-Lookupzone mit A-Einträgen und eine Reverse-Lookupzone mit PTR-Einträgen, die für jede VCF-Verwaltungs-Appliance in jeder EVS-Bereitstellung erstellt wurden.	10.1.5.13	cb01

Komponente	Description	Mindestanforderungen	Beispiel für eine IP-Adresse	Beispiel für einen Hostnamen
NSX Edge 1-Appliance	IP-Adresse und Hostname, die im A-Datensatz und im PTR-Datensatz für die NSX Edge 1-Appliance definiert sind.	Amazon EVS benötigt eine DNS-Forward-Lookupzone mit A-Einträgen und eine Reverse-Lookupzone mit PTR-Einträgen, die für jede VCF-Verwaltungs-Appliance in jeder EVS-Bereitstellung erstellt wurden.	10.1.5.14	Rand 01
NSX Edge 2-Appliance	IP-Adresse und Hostname, die im A-Datensatz und im PTR-Datensatz für die NSX Edge 2-Appliance definiert sind.	Amazon EVS benötigt eine DNS-Forward-Lookupzone mit A-Einträgen und eine Reverse-Lookupzone mit PTR-Einträgen, die für jede VCF-Verwaltungs-Appliance in jeder EVS-Bereitstellung erstellt wurden.	10.1.5.15	Rand 02

Komponente	Description	Mindestanforderungen	Beispiel für eine IP-Adresse	Beispiel für einen Hostnamen
NSX Manager 1-Appliance	IP-Adresse und Hostname, die im A-Datensatz und im PTR-Datensatz für die NSX Manager 1-Appliance definiert sind.	Amazon EVS benötigt eine DNS-Forward-Lookupzone mit A-Einträgen und eine Reverse-Lookupzone mit PTR-Einträgen, die für jede VCF-Verwaltungs-Appliance in jeder EVS-Bereitstellung erstellt wurden.	10.1.5.16	nsx 01
NSX Manager 2-Appliance	IP-Adresse und Hostname, die im A-Datensatz und im PTR-Datensatz für die NSX Manager 2-Appliance definiert sind.	Amazon EVS benötigt eine DNS-Forward-Lookupzone mit A-Einträgen und eine Reverse-Lookupzone mit PTR-Einträgen, die für jede VCF-Verwaltungs-Appliance in jeder EVS-Bereitstellung erstellt wurden.	10.1.5.17	nsx 02

Komponente	Description	Mindestanforderungen	Beispiel für eine IP-Adresse	Beispiel für einen Hostnamen
NSX Manager 3-Appliance	IP-Adresse und Hostname, die im A-Datensatz und im PTR-Datensatz für die NSX Manager 3-Appliance definiert sind.	Amazon EVS benötigt eine DNS-Forward-Lookupzone mit A-Einträgen und eine Reverse-Lookupzone mit PTR-Einträgen, die für jede VCF-Verwaltungs-Appliance in jeder EVS-Bereitstellung erstellt wurden.	10.1.5.18	nsx 03

VPC-Routenserver-Infrastruktur

Komponente	Description	Mindestanforderungen	Beispielwert (e)
Route-Server-ID	Amazon EVS verwendet Amazon VPC Route Server, um BGP-basiertes dynamisches Routing zu Ihrem VPC-Underlay-Netzwerk zu ermöglichen.	Sie müssen einen Routenserver angeben, der Routen mit mindestens zwei Route-Server-Endpunkten im Service-Access-Subnetz teilt. Die auf dem Routenserver konfigurierte Peer-ASN und der NSX Edge-Peer müssen übereinstimmen, und	rs-0a1b2c3d4e5f67890

Komponente	Description	Mindestanforderungen	Beispielwert (e)
		die Peer-IP-Adressen müssen eindeutig sein.	

Route-Server-Zuordnung	Die Verbindung zwischen einem Routenserver und einer VPC.	Ihr Routenserver muss mit Ihrer VPC verknüpft sein.	<pre>{
			"RouteServerAssociation": {
			"RouteServerId": "rs-0a1b2c3d4e5f67890",
			"VpcId": "vpc-1",
			"State": "associating"
			}
			}</pre>

BGP ASN der VPC-Route-Server-Seite (Amazon-seitige ASN)	Die Amazon-seitige ASN stellt die AWS Seite der BGP-Sitzung zwischen dem VPC-Routenserver und dem NSX Edge-Peer dar. Sie geben diese BGP ASN, wenn Sie den Routenserver erstellen. Weitere Informationen finden Sie unter Erstellen eines Routenservers im Amazon VPC-Benutzerhandbuch.	Dieser Wert muss eindeutig sein und im Bereich von 1-4294967295 liegen. AWS empfiehlt die Verwendung einer privaten ASN im Bereich 64512—65534 (16-Bit-ASN) oder 4200000000—4294967294 (32-Bit-ASN).	65001

Komponente	Description	Mindestanforderungen	Beispielwert (e)
ID des Route-Serverendpunkts 1	Ein Routenserver-Endpunkt ist eine AWS verwaltete Komponente innerhalb eines Subnetzes, die BGP-Verbindungen (Border Gateway Protocol) zwischen Ihrem Routenserver und Ihren BGP-Peers ermöglicht.	Der Routenserver-Endpunkt muss im Servicezugriffssubnetz bereitgestellt werden.	rse-0123456789abcdef0
Route-Server-Peer 1 ID	Der Routenserver-Peer ist eine BGP-Peering-Sitzung zwischen einem Routenserver-Endpunkt und dem in AWS (NSX Edge) bereitgestellten Gerät.	Der im Routenserver-Peer angegebene Peer-ASN-Wert muss mit dem Peer-ASN-Wert übereinstimmen, der für das NSX Edge Tier-0-Gateway verwendet wird.	rsp-0123456789abcdef0
Peer-1-IP-Adresse des Routenservers (EVS NSX Edge 1-Seite)	Die IP-Adresse des Routenserver-Peers (`PeerAddress`).	Muss eine eindeutige, ungenutzte IP-Adresse aus dem NSX-Uplink-VLAN verwenden. Amazon EVS wendet diese IP-Adresse im Rahmen der Bereitstellung auf NSX Edge 1 an und führt einen Peer mit dem Route-Server-Endpunkt-Peer durch.	10.1.7.10

Komponente	Description	Mindestanforderungen	Beispielwert (e)
ENI-Adresse des Route-Server-Peer-1-Endpunkts	Die ENI-Endpunkt-IP-Adresse des Route-Server-Peers (`EndpointEniAddress`).	Wird automatisch vom Routenserver bei der Peer-Erstellung generiert.	10.1.7.11
ID des Endpunkts 2 des Routenservers	Ein Routenserver-Endpunkt ist eine AWS verwaltete Komponente innerhalb eines Subnetzes, die BGP-Verbindungen (Border Gateway Protocol) zwischen Ihrem Routenserver und Ihren BGP-Peers ermöglicht.	Der Routenserver-Endpunkt muss im Servicezugriffssubnetz bereitgestellt werden.	rse-fedcba9876543210f
Peer-2-ID des Routenservers (EVS NSX Edge 2-Seite)	Der Routenserver-Peer ist eine BGP-Peering-Sitzung zwischen einem Routenserver-Endpunkt und dem in AWS (NSX Edge) bereitgestellten Gerät.	Der im Routenserver-Peer angegebene Peer-ASN-Wert muss mit dem Peer-ASN-Wert übereinstimmen, der für das NSX Edge Tier-0-Gateway verwendet wird.	rsp-fedcba9876543210f

Komponente	Description	Mindestanforderungen	Beispielwert (e)
IP-Adresse des Routenservers (Peer 2)	Die IP-Adresse des Route-Server-Peers (`PeerAddress`).	Muss eine eindeutige IP-Adresse aus dem NSX-Uplink-VLAN verwenden. Amazon EVS wendet diese IP-Adresse im Rahmen der Bereitstellung auf NSX Edge 2 an und führt einen Peer mit dem Route-Server-Endpunkt-Peer durch.	10.1.7.200
ENI-Adresse des Route-Server-Peer-2-Endpunkts	Die ENI-Endpunkt-IP-Adresse des Route-Server-Peers (`EndpointEniAddress`).	Wird automatisch vom Routenserver bei der Peer-Erstellung generiert.	10.1.7.201
Route-Server-Ausbreitung	Bei der Route-Server-Propagierung werden die Routen in der FIB in der von Ihnen angegebenen Routentabelle installiert.	Sie müssen die Routentabelle angeben, die Ihrem Servicezugriffs-Subnetz zugeordnet ist. Amazon EVS unterstützt IPv4 derzeit nur Netzwerke.	{ "RouteServerEndpoint": { "RouteServerId": "rs-1", "RouteServerEndpointId": "rse-1", "VpcId": "vpc-1", "SubnetId": "subnet-1", "State": "pending" } }

Komponente	Description	Mindestanforderungen	Beispielwert (e)
BGP ASN der NSX-Peer-Seite	BGP ASN für die NSX-Seite der Verbindung.	Schlagen Sie vor, die NSX-Standard-ASN 65000 zu verwenden	65000

HCX-Ressourcen für den Internetzugang (optional)

Komponente	Description	Mindestanforderungen	Beispielwert (e)
IPAM-ID	Amazon VPC IP Address Manager (IPAM) wird zur Verwaltung von IP-Adressen für den HCX-Internetzugang verwendet.	Muss für die Bereitstellung öffentlicher Adressen konfiguriert werden. IPv4 Nur für die Konfiguration des HCX-Internetzugangs erforderlich.	ipam-0123456789abcdef0
IPAM-Pool-ID	Ein öffentlicher IPv4 IPAM-Pool im Besitz von Amazon, der Adressen für HCX-Komponenten bereitstellt.	Muss als öffentlicher Pool konfiguriert werden. IPv4 Nur für die Konfiguration des HCX-Internetzugangs erforderlich.	ipam-pool-0123456789abcdef0
Öffentlicher HCX-VLAN-CIDR-Block	Ein sekundärer öffentlicher IPv4 CIDR-Block, der aus dem IPAM-Pool für das öffentliche HCX-VLAN-Subnetz zugewiesen wurde.	Muss über eine /28-Netzmaske verfügen und aus dem öffentlichen IPAM-Pool von Amazon zugewiesen werden. Nur für die Konfiguration des HCX-Internetzugangs erforderlich.	18.97.137.0/28

Komponente	Description	Mindestanforderungen	Beispielwert (e)
Elastic-IP-Adressen	Sequentielle Elastic IP-Adressen, die aus dem IPAM-Pool für HCX-Komponenten zugewiesen wurden.	Mindestens 3 EIPs aus demselben IPAM-Pool für HCX Manager, HCX Interconnect Appliance (HCX-IX) und HCX Network Extension (HCX-NE). Nur für die HCX-Internetzugangskonfiguration erforderlich.	eipalloc-0123456789abcdef0, eipalloc-0123456789abcdef1, eipalloc-0123456789abcdef2

Erste Schritte mit Amazon Elastic VMware Service

Verwenden Sie dieses Handbuch, um mit Amazon Elastic VMware Service (Amazon EVS) zu beginnen. Sie erfahren, wie Sie eine Amazon EVS-Umgebung mit Hosts in Ihrer eigenen Amazon Virtual Private Cloud (VPC) erstellen.

Wenn Sie fertig sind, verfügen Sie über eine Amazon EVS-Umgebung, mit der Sie Ihre VMware vSphere-basierten Workloads auf die migrieren können. AWS Cloud

> **Important**
>
> Um den Einstieg so einfach und schnell wie möglich zu gestalten, enthält dieses Thema Schritte zum Erstellen einer VPC und legt die Mindestanforderungen für die DNS-Serverkonfiguration und die Erstellung einer Amazon EVS-Umgebung fest. Bevor Sie diese Ressourcen erstellen, empfehlen wir Ihnen, Ihren IP-Adressraum und die Einrichtung Ihres DNS-Eintrags so zu planen, dass sie Ihren Anforderungen entsprechen. Sie sollten sich auch mit den Anforderungen von VCF 5.2.x vertraut machen. In den Versionshinweisen zu VCF 5.2.x finden Sie relevante Versionsinformationen.

> **Important**
>
> Informationen zu den von Amazon EVS bereitgestellten VCF-Versionen finden Sie unter. the section called “VCF-Versionen und EC2-Instances”

Themen

Voraussetzungen

Bevor Sie beginnen, müssen Sie die erforderlichen Aufgaben für Amazon EVS abschließen. Weitere Informationen finden Sie unter Amazon Elastic VMware Service einrichten.

Erstellen Sie eine VPC mit Subnetzen und Routentabellen

> **Note**
>
> Die VPC, die Subnetze und die Amazon EVS-Umgebung müssen alle im selben Konto erstellt werden. Amazon EVS unterstützt keine kontenübergreifende gemeinsame Nutzung von VPC-Subnetzen oder Amazon EVS-Umgebungen.

Example

Amazon VPC console

1. Öffnen Sie die Amazon VPC -Konsole.
2. Wählen Sie auf dem VPC-Dashboard Create VPC (VPC erstellen) aus.
3. Wählen Sie unter Zu erstellende Ressourcen die Option VPC und mehr aus.
4. Lassen Sie die automatische Generierung von Namenstags aktiviert, um Namenstags für die VPC-Ressourcen zu erstellen, oder deaktivieren Sie sie, um Ihre eigenen Namenstags für die VPC-Ressourcen bereitzustellen.
5. Geben Sie für IPv4 CIDR-Block einen CIDR-Block ein. IPv4 Eine VPC muss über einen IPv4 CIDR-Block verfügen. Stellen Sie sicher, dass Sie eine VPC erstellen, die ausreichend dimensioniert ist, um die Amazon EVS-Subnetze aufzunehmen. Weitere Informationen finden Sie unter the section called “Überlegungen zum Amazon EVS-Netzwerk”.

> **Note**
>
> Amazon EVS unterstützt IPv6 derzeit nicht.

6. Behalten Sie das Mietverhältnis bei als. `Default` Wenn diese Option ausgewählt ist, verwenden EC2-Instances, die in dieser VPC gestartet werden, das Tenancy-Attribut, das beim Start der Instances angegeben wurde. Amazon EVS startet Bare-Metal-EC2-Instances in Ihrem Namen.
7. Wählen Sie für Number of Availability Zones (AZs) die Option 1 aus.

> **Note**
>
> Amazon EVS unterstützt derzeit nur Single-AZ-Bereitstellungen.

8. Erweitern Sie Anpassen AZs und wählen Sie die AZ für Ihre Subnetze aus.

> **Note**
>
> Sie müssen in einer AWS Region bereitstellen, in der Amazon EVS unterstützt wird. Weitere Informationen zur Verfügbarkeit von Amazon EVS in der Region finden Sie unter Amazon Elastic VMware Service Endpoints and Quotas im AWS General Reference Guide.

9. (Optional) Wenn Sie eine Internetverbindung benötigen, wählen Sie für Anzahl der öffentlichen Subnetze die Option 1.
10. Wählen Sie für Anzahl der privaten Subnetze den Wert 1 aus. Dieses private Subnetz wird als Subnetz für den Servicezugriff verwendet, das Sie Amazon EVS bei der Erstellung der Umgebung zur Verfügung gestellt haben. Weitere Informationen finden Sie unter the section called “Subnetz für den Servicezugriff”.
11. Um die IP-Adressbereiche für Ihre Subnetze auszuwählen, erweitern Sie die Option CIDR-Blöcke für Subnetze anpassen.

> **Note**
>
> Amazon EVS-VLAN-Subnetze müssen ebenfalls aus diesem VPC-CIDR-Bereich erstellt werden. Stellen Sie sicher, dass Sie im VPC-CIDR-Block genügend Speicherplatz für die VLAN-Subnetze lassen, die der Dienst benötigt. Weitere

Informationen finden Sie unter the section called “Überlegungen zum Amazon EVS-Netzwerk”.

12. (Optional) Um Internetzugriff auf Ressourcen IPv4 zu gewähren, wählen Sie für NAT-Gateways In 1 AZ aus. Beachten Sie, dass für NAT-Gateways Kosten anfallen. Weitere Informationen finden Sie unter Preise für NAT-Gateways.

> **Note**
>
> Amazon EVS erfordert die Verwendung eines NAT-Gateways, um ausgehende Internetkonnektivität zu ermöglichen.

13. Wählen Sie für VPC endpoints (VPC-Endpunkte) None (Keine) aus.

> **Note**
>
> Amazon EVS unterstützt derzeit keine Gateway-VPC-Endpunkte. Amazon S3 Um Amazon S3 Konnektivität zu aktivieren, müssen Sie mit AWS PrivateLink for Amazon S3 einen VPC-Schnittstellen-Endpunkt einrichten. Weitere Informationen finden Sie unter AWS PrivateLink für Amazon S3 im Amazon Simple Storage Service-Benutzerhandbuch.

14. Behalten Sie für DNS-Optionen die ausgewählten Standardeinstellungen bei. Amazon EVS setzt voraus, dass Ihre VPC über DNS-Auflösungsfunktionen für alle VCF-Komponenten verfügt.
15. (Optional) Um ein Tag zu Ihrer VPC hinzuzufügen, erweitern Sie Zusätzliche Tags, wählen Sie Neues Tag hinzufügen, und geben Sie einen Tag-Schlüssel und einen Tag-Wert ein.
16. Wählen Sie VPC erstellen aus.

> **Note**
>
> Erstellt während der VPC-Erstellung Amazon VPC automatisch eine Haupt-Routing-Tabelle und ordnet ihr standardmäßig implizit Subnetze zu.

AWS CLI

1. Öffnen Sie eine Terminalsitzung.

2. Erstellen Sie eine VPC mit einem privaten Subnetz und einem optionalen öffentlichen Subnetz in einer einzigen Availability Zone.

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

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

3. Aktiviert DNS-Hostnamen und DNS-Unterstützung.

```
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. Erstellen Sie ein privates Subnetz in der 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. Speichern Sie die private Subnetz-ID zur Verwendung in nachfolgenden Befehlen.

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

6. (Optional) Erstellen Sie ein öffentliches Subnetz, falls eine Internetverbindung erforderlich ist.

```
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. (Optional) Speichern Sie die öffentliche Subnetz-ID zur Verwendung in nachfolgenden Befehlen.

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

8. (Optional) Erstellen Sie ein Internet-Gateway und schließen Sie es an, wenn das öffentliche Subnetz erstellt wird.

```
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. (Optional) Erstellen Sie ein NAT-Gateway, falls eine Internetverbindung erforderlich ist.

```
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. Erstellen und konfigurieren Sie die erforderlichen Routing-Tabellen.

```
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. Fügen Sie die erforderlichen Routen zu den Routentabellen hinzu.

```
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. Ordnen Sie die Routing-Tabellen Ihren Subnetzen zu.

```
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**
>
> Erstellt während der VPC-Erstellung Amazon VPC automatisch eine Haupt-Routing-Tabelle und ordnet ihr standardmäßig implizit Subnetze zu.

Wählen Sie Ihre HCX-Konnektivitätsoption

Wählen Sie eine Verbindungsoption für Ihre Amazon EVS-Umgebung aus:

- Private Konnektivität: Stellt leistungsstarke Netzwerkpfade für HCX bereit und optimiert so Zuverlässigkeit und Konsistenz. Erfordert die Verwendung von AWS Direct Connect oder Site-to-Site VPN für externe Netzwerkkonnektivität.
- Internetkonnektivität: Nutzt das öffentliche Internet, um einen flexiblen Migrationspfad einzurichten, der schnell eingerichtet werden kann. Erfordert die Verwendung von VPC IP Address Manager (IPAM) und Elastic IP-Adressen.

Eine ausführliche Analyse finden Sie unter. the section called “HCX-Konnektivitätsoptionen”

Wählen Sie Ihre Option:

- Option A: Nur private Konnektivität → Weiter zuthe section called “Konfigurieren Sie die VPC-Hauptroutentabelle”.
- Option B: Internetverbindung → Weiter zuthe section called “Einrichtung der HCX-Internetverbindung”.

Einrichtung der HCX-Internetverbindung

> **Note**
>
> Überspringen Sie diesen Abschnitt, wenn Sie sich für private HCX-Konnektivität entschieden haben, und fahren Sie fort. the section called “Konfigurieren Sie die VPC-Hauptroutentabelle”

Um die HCX-Internetverbindung für Amazon EVS zu aktivieren, müssen Sie:

- Stellen Sie sicher, dass Ihr IPAM-Kontingent (VPC IP Address Manager) für von Amazon bereitgestellte zusammenhängende öffentliche IPv4 CIDR-Blocknetzmasken mindestens /28 beträgt.

  > **Important**
  >
  > Die Verwendung eines von Amazon bereitgestellten zusammenhängenden öffentlichen IPv4 CIDR-Blocks mit einer Netzmaskenlänge von weniger als /28 führt zu HCX-Konnektivitätsproblemen. Weitere Informationen zur Erhöhung der IPAM-Kontingente finden Sie unter Kontingente für Ihr IPAM.

- Erstellen Sie einen IPAM und einen öffentlichen IPv4 IPAM-Pool mit einem CIDR, der eine Mindestnetzmaskenlänge von /28 hat.
- Weisen Sie den HCX Manager- und HCX Interconnect (HCX-IXEIPs) -Appliances mindestens zwei Elastic IP-Adressen () aus dem IPAM-Pool zu. Weisen Sie jeder HCX-Netzwerk-Appliance, die Sie bereitstellen müssen, eine zusätzliche Elastic IP-Adresse zu.
- Fügen Sie den öffentlichen IPv4 CIDR-Block als zusätzlichen CIDR zu Ihrer VPC hinzu.

Weitere Informationen zur Verwaltung der HCX-Internetkonnektivität nach der Erstellung der Umgebung finden Sie unter. the section called “Öffentliche HCX-Konnektivität”

Erstellen Sie ein IPAM

Gehen Sie wie folgt vor, um ein IPAM zu erstellen.

> **Note**
>
> Sie können das kostenlose Kontingent für IPAM verwenden, um IPAM-Ressourcen für die Verwendung mit Amazon EVS zu erstellen. IPAM selbst ist im Rahmen des kostenlosen Kontingents zwar kostenlos, Sie sind jedoch für die Kosten anderer AWS Dienste verantwortlich, die in Verbindung mit IPAM genutzt werden, wie z. B. NAT-Gateways und alle öffentlichen IPv4 Adressen, die Sie verwenden und die über das kostenlose Kontingent hinausgehen. Weitere Informationen zu den IPAM-Preisen finden Sie auf der Preisseite.Amazon VPC

> **Note**
>
> Amazon EVS unterstützt derzeit keine private IPv6 Global Unicast Address (GUA) CIDRs .

Erstellen Sie einen öffentlichen IPAM-Pool IPv4

Gehen Sie wie folgt vor, um einen öffentlichen IPv4 Pool zu erstellen.

IPAM console

1. Öffnen Sie die IAM-Konsole.
2. Wählen Sie im Navigationsbereich Pools aus.
3. Wählen Sie den Bereich Öffentlich. Weitere Informationen zu Bereichen finden Sie unter So funktioniert IPAM.
4. Wählen Sie Pool erstellen.
5. (Optional) Fügen Sie ein Namens-Tag für den Pool und eine Beschreibung für den Pool hinzu.
6. Wählen Sie unter Adressfamilie die Option aus. IPv4
7. Belassen Sie unter Ressourcenplanung den IP-Bereich für den Plan innerhalb des ausgewählten Bereichs ausgewählt.
8. Wählen Sie unter Gebietsschema das Gebietsschema für den Pool aus. Das Gebietsschema ist die AWS Region, in der dieser IPAM-Pool für Zuweisungen verfügbar sein soll. Das von Ihnen gewählte Gebietsschema muss der AWS Region entsprechen, in der Ihre VPC bereitgestellt wird.

9. Wählen Sie unter Dienst EC2 (EIP/VPC) aus. Dadurch werden CIDRs angekündigt, die aus diesem Pool für den Amazon EC2-Service (für Elastic IP-Adressen) zugewiesen wurden.
10. Wählen Sie unter Öffentliche IP-Quelle die Option Amazon-eigen aus.
11. Wählen CIDRs Sie unter Bereitstellung die Option Öffentliche CIDR im Besitz von Amazon hinzufügen aus.
12. Wählen Sie unter Netzmaske eine CIDR-Netzmaskenlänge aus. /28 ist die erforderliche Mindestlänge der Netzmaske.
13. Wählen Sie Pool erstellen.

AWS CLI

1. Öffnen Sie eine Terminalsitzung.
2. Rufen Sie die Public Scope-ID von Ihrem IPAM ab.

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

3. Erstellen Sie einen IPAM-Pool im öffentlichen Bereich.

```
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. Speichern Sie die Pool-ID zur Verwendung in nachfolgenden Befehlen.

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

5. Stellen Sie einen CIDR-Block aus dem Pool mit einer Mindestnetzmaskenlänge von /28 bereit.

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

Weisen Sie Elastic IP-Adressen aus dem IPAM-Pool zu

Gehen Sie wie folgt vor, um Elastic IP-Adressen (EIPs) aus dem IPAM-Pool für HCX Service Mesh-Appliances zuzuweisen.

Amazon VPC console

1. Öffnen Sie die Amazon VPC-Konsole.
2. Wählen Sie im Navigationsbereich Elastic aus. IPs
3. Wählen Sie Elastic-IP-Adresse zuweisen aus.
4. Wählen Sie Mit einem IPv4 IPAM-Pool zuweisen aus.
5. Wählen Sie den öffentlichen IPv4 Pool von Amazon aus, den Sie zuvor konfiguriert haben.
6. Wählen Sie unter IPAM-Methode zuweisen die Option Adresse im IPAM-Pool manuell eingeben aus.

> **Important**
>
> Sie können die ersten beiden EIPs oder die letzten EIP aus dem öffentlichen IPAM-CIDR-Block nicht dem VLAN-Subnetz zuordnen. Diese EIPs sind als Netzwerk-, Standard-Gateway- und Broadcast-Adressen reserviert. Amazon EVS gibt einen Validierungsfehler aus, wenn Sie versuchen, diese EIPs dem VLAN-Subnetz zuzuordnen.

> **Important**
>
> Geben Sie Adressen innerhalb des IPAM-Pool manuell ein, um sicherzustellen, EIPs dass die Amazon EVS-Reserven nicht zugewiesen werden. Wenn Sie IPAM die Wahl der EIP gestatten, weist IPAM möglicherweise eine EIP zu, die Amazon EVS reserviert, was zu einem Fehler bei der EIP-Zuordnung zum VLAN-Subnetz führt.

7. Geben Sie die EIP an, die aus dem IPAM-Pool zugewiesen werden soll.
8. Wählen Sie Allocate aus.
9. Wiederholen Sie diesen Vorgang, um den Rest EIPs zuzuweisen, den Sie benötigen. Sie müssen den HCX Manager- und HCX Interconnect (HCX-IX) Appliances mindestens zwei EIPs aus dem IPAM-Pool zuweisen. Weisen Sie jeder HCX-Netzwerk-Appliance, die Sie bereitstellen müssen, eine zusätzliche EIP zu.

AWS CLI

1. Öffnen Sie eine Terminalsitzung.
2. Rufen Sie die IPAM-Pool-ID ab, die Sie zuvor erstellt haben.

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

3. Weisen Sie Elastic IP-Adressen aus dem IPAM-Pool zu. Sie müssen den HCX Manager- und HCX Interconnect (HCX-IX) Appliances mindestens zwei EIPs aus dem IPAM-Pool zuweisen. Weisen Sie jeder HCX-Netzwerk-Appliance, die Sie bereitstellen müssen, eine zusätzliche EIP zu.

> **Important**
>
> Sie können die ersten beiden EIPs oder die letzten EIP aus dem öffentlichen IPAM-CIDR-Block nicht einem VLAN-Subnetz zuordnen. Diese EIPs sind als Netzwerk-, Standard-Gateway- und Broadcast-Adressen reserviert. Amazon EVS gibt einen Validierungsfehler aus, wenn Sie versuchen, diese EIPs dem VLAN-Subnetz zuzuordnen.

> **Important**
>
> Geben Sie Adressen innerhalb des IPAM-Pool manuell ein, um sicherzustellen, EIPs dass die Amazon EVS-Reserven nicht zugewiesen werden. Wenn Sie IPAM die Wahl der EIP gestatten, weist IPAM möglicherweise eine EIP zu, die Amazon EVS reserviert, was zu einem Fehler bei der EIP-Zuordnung zum VLAN-Subnetz führt.

```
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
```

Fügen Sie den öffentlichen IPv4 CIDR-Block aus dem IPAM-Pool zur VPC für HCX-Internetkonnektivität hinzu

Um die HCX-Internetverbindung zu aktivieren, müssen Sie den öffentlichen IPv4 CIDR-Block aus dem IPAM-Pool als zusätzlichen CIDR zu Ihrer VPC hinzufügen. Amazon EVS verwendet diesen CIDR-Block, um VMware HCX mit Ihrem Netzwerk zu verbinden. Gehen Sie wie folgt vor, um den CIDR-Block zu Ihrer VPC hinzuzufügen.

> **Important**
>
> Sie müssen den IPv4 CIDR-Block, den Sie Ihrer VPC hinzufügen, manuell eingeben. Amazon EVS unterstützt derzeit nicht die Verwendung eines IPAM-zugewiesenen CIDR-Blocks. Die Verwendung eines IPAM-zugewiesenen CIDR-Blocks kann zu einem Fehler bei der EIP-Zuordnung führen.

Amazon VPC console

1. Öffnen Sie die Amazon VPC-Konsole.
2. Wählen Sie im Navigationsbereich Ihr aus. VPCs
3. Wählen Sie die VPC aus, die Sie zuvor erstellt haben, und wählen Sie Aktionen, Bearbeiten CIDRs.
4. Wählen Sie Neues IPV4 CIDR hinzufügen aus.
5. Wählen Sie Manuelle IPV4 CIDR-Eingabe aus.
6. Geben Sie den CIDR-Block aus dem öffentlichen IPAM-Pool an, den Sie zuvor erstellt haben.

AWS CLI

1. Öffnen Sie eine Terminalsitzung.
2. Rufen Sie die IPAM-Pool-ID und den bereitgestellten CIDR-Block ab.

```
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. Fügen Sie den CIDR-Block zu Ihrer VPC hinzu.

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

Konfigurieren Sie die VPC-Hauptroutentabelle

Amazon EVS-VLAN-Subnetze sind implizit der VPC-Hauptroutentabelle zugeordnet. Um die Konnektivität zu abhängigen Diensten wie DNS oder lokalen Systemen für eine erfolgreiche Implementierung der Umgebung zu aktivieren, müssen Sie die Haupt-Routing-Tabelle so konfigurieren, dass Datenverkehr zu diesen Systemen zugelassen wird. Die Hauptroutentabelle

muss eine Route für das CIDR der VPC enthalten. Die Verwendung der Haupt-Routing-Tabelle ist nur für die erste Bereitstellung der Amazon EVS-Umgebung erforderlich. Nach der Bereitstellung der Umgebung können Sie Ihre Umgebung so konfigurieren, dass sie eine benutzerdefinierte Routing-Tabelle verwendet. Weitere Informationen finden Sie unter the section called “Konfigurieren Sie eine benutzerdefinierte Routentabelle”.

Nach der Bereitstellung der Umgebung müssen Sie jedes der Amazon EVS-VLAN-Subnetze explizit einer Routing-Tabelle in Ihrer VPC zuordnen. Die NSX-Konnektivität schlägt fehl, wenn Ihre VLAN-Subnetze nicht explizit einer VPC-Routentabelle zugeordnet sind. Wir empfehlen dringend, dass Sie Ihre Subnetze nach der Bereitstellung der Umgebung explizit einer benutzerdefinierten Routentabelle zuordnen. Weitere Informationen finden Sie unter the section called “Konfigurieren Sie die VPC-Hauptroutentabelle”.

> **Important**
>
> Amazon EVS unterstützt die Verwendung einer benutzerdefinierten Routentabelle erst, nachdem die Amazon EVS-Umgebung erstellt wurde. Benutzerdefinierte Routing-Tabellen sollten bei der Erstellung der Amazon EVS-Umgebung nicht verwendet werden, da dies zu Verbindungsproblemen führen kann.

Konfigurieren von DNS- und NTP-Servern mithilfe des VPC-DHCP-Optionssatzes

> **Important**
>
> Ihre Umgebungsbereitstellung schlägt fehl, wenn Sie die folgenden Amazon EVS-Anforderungen nicht erfüllen:
>
> - Nehmen Sie eine primäre DNS-Server-IP-Adresse und eine sekundäre DNS-Server-IP-Adresse in den DHCP-Optionssatz auf.
> - Fügen Sie eine DNS-Forward-Lookupzone mit A-Einträgen für jede VCF-Verwaltungs-Appliance und jeden Amazon EVS-Host in Ihre Bereitstellung ein.
> - Fügen Sie eine DNS-Reverse-Lookupzone mit PTR-Einträgen für jede VCF-Verwaltungs-Appliance und jeden Amazon EVS-Host in Ihre Bereitstellung ein.
> - Konfigurieren Sie die Haupt-Routing-Tabelle der VPC, um sicherzustellen, dass eine Route zu Ihren DNS-Servern vorhanden ist.

- Stellen Sie sicher, dass Ihre Domainnamenregistrierung gültig und nicht abgelaufen ist, und dass keine doppelten Hostnamen oder IP-Adressen vorhanden sind.
- Konfigurieren Sie Ihre Sicherheitsgruppen und Netzwerk-Zugriffskontrolllisten (ACLs), damit Amazon EVS kommunizieren kann mit:
  - DNS-Server über TCP/UDP Port 53.
  - Host-Management-VLAN-Subnetz über HTTPS und SSH.
  - Verwaltungs-VLAN-Subnetz über HTTPS und SSH.

Amazon EVS verwendet den DHCP-Optionssatz Ihrer VPC, um Folgendes abzurufen:

- DNS-Server (Domain Name System) für die Auflösung von Host-IP-Adressen.
- Domainnamen für die DNS-Auflösung.
- NTP-Server (Network Time Protocol) für die Zeitsynchronisierung.

Sie können einen DHCP-Optionssatz mit der Amazon VPC Konsole oder erstellen. AWS CLI Weitere Informationen finden Sie im Amazon VPC Benutzerhandbuch unter Erstellen eines DHCP-Optionssatzes.

DNS-Server konfigurieren

Die DNS-Konfiguration ermöglicht die Hostnamenauflösung in Ihrer Amazon EVS-Umgebung. Um eine Amazon EVS-Umgebung erfolgreich bereitzustellen, muss der DHCP-Optionssatz Ihrer VPC über die folgenden DNS-Einstellungen verfügen:

- Eine primäre DNS-Server-IP-Adresse und eine sekundäre DNS-Server-IP-Adresse im DHCP-Optionssatz.
- Eine DNS-Forward-Lookupzone mit A-Einträgen für jede VCF-Verwaltungs-Appliance und jeden Amazon EVS-Host in Ihrer Bereitstellung.
- Eine Reverse-Lookupzone mit PTR-Datensätzen für jede VCF-Verwaltungs-Appliance und jeden Amazon EVS-Host in Ihrer Bereitstellung. Für die NTP-Konfiguration können Sie die standardmäßige Amazon NTP-Adresse oder eine andere IPv4 Adresse verwenden`169.254.169.123`, die Sie bevorzugen.

Weitere Informationen zur Konfiguration von DNS-Servern in einem DHCP-Optionssatz finden Sie unter Einen DHCP-Optionssatz erstellen.

Konfigurieren Sie DNS für lokale Konnektivität

Für lokale Konnektivität empfehlen wir die Verwendung von privaten gehosteten Route 53 53-Zonen mit eingehenden Resolvern. Dieses Setup ermöglicht die Hybrid-DNS-Auflösung, bei der Sie Route 53 für internes DNS innerhalb Ihrer VPC verwenden und es in Ihre bestehende lokale DNS-Infrastruktur integrieren können. Auf diese Weise können Ressourcen in Ihrer VPC Domainnamen auflösen, die in Ihrem lokalen Netzwerk gehostet werden, und umgekehrt, ohne dass komplexe Konfigurationen erforderlich sind. Bei Bedarf können Sie auch Ihren eigenen DNS-Server mit Route 53 53-Outbound-Resolvern verwenden. Schritte zur Konfiguration finden Sie unter Erstellen einer privaten gehosteten Zone und Weiterleiten eingehender DNS-Abfragen an Ihre VPC im Amazon Route 53 53-Entwicklerhandbuch.

> **Note**
>
> Die Verwendung sowohl von Route 53 als auch eines benutzerdefinierten DNS-Servers (Domain Name System) im DHCP-Optionssatz kann zu unerwartetem Verhalten führen.

> **Note**
>
> Wenn Sie benutzerdefinierte DNS-Domänennamen verwenden, die in einer privaten gehosteten Zone definiert sind Route 53, oder privates DNS mit VPC-Endpunkten (AWS PrivateLink) der Schnittstelle verwenden, müssen Sie `enableDnsHostnames` sowohl die `enableDnsSupport` Attribute als auch auf festlegen. `true` Weitere Informationen finden Sie unter DNS-Attribute für Ihre VPC.

Beheben Sie Probleme mit der DNS-Erreichbarkeit

Amazon EVS benötigt eine persistente Verbindung zu SDDC Manager und DNS-Servern im DHCP-Optionssatz Ihrer VPC, um DNS-Einträge zu erreichen. Wenn die persistente Verbindung zu SDDC Manager nicht mehr verfügbar ist, kann Amazon EVS den Umgebungsstatus nicht mehr überprüfen, und Sie verlieren möglicherweise den Zugriff auf die Umgebung. Schritte zur Behebung dieses Problems finden Sie unter. the section called “Die Erreichbarkeitsprüfung ist fehlgeschlagen”

NTP-Server konfigurieren

NTP-Server stellen die Zeit in Ihrem Netzwerk bereit. Eine konsistente und genaue Zeitreferenz auf Ihrer Amazon EC2 EC2-Instance ist für viele Aufgaben und Prozesse in der VCF-Umgebung von entscheidender Bedeutung. Die Zeitsynchronisierung ist wichtig für:

- Systemprotokollierung und Prüfung
- Sicherheitsvorgänge
- Verteilte Systemverwaltung
- Fehlerbehebung

Sie können die IPv4 Adressen von bis zu vier NTP-Servern in den DHCP-Optionssatz Ihrer VPC eingeben. Sie können den Amazon Time Sync Service unter der IPv4 Adresse angeben`169.254.169.123`. Standardmäßig verwenden die Amazon EC2 EC2-Instances, die Amazon EVS bereitstellt, den Amazon Time Sync Service an der Adresse. IPv4 `169.254.169.123`

Weitere Informationen zu NTP-Servern finden Sie unter RFC 2123. Weitere Informationen zu Amazon Time Sync Service finden Sie unter Präzise Uhr- und Uhrzeitsynchronisierung in Ihrer EC2-Instance und Konfigurieren von NTP auf VMware Cloud Foundation-Hosts in der VMware Cloud Foundation-Dokumentation.

Um NTP-Einstellungen zu konfigurieren

1. Wählen Sie Ihre NTP-Quelle:
   - Amazon Time Sync Service (empfohlen)
   - Benutzerdefinierte NTP-Server
2. Fügen Sie NTP-Server zu Ihrem DHCP-Optionssatz hinzu. Weitere Informationen finden Sie unter Erstellen eines DHCP-Optionssatzes im Amazon VPC-Benutzerhandbuch.
3. Überprüfen Sie die Zeitsynchronisierung. Weitere Hinweise zur Konfiguration des DHCP-Optionssatzes finden Sie unterthe section called “Konfigurieren Sie den DHCP-Optionssatz Ihrer VPC”.

Konfigurieren Sie die lokale Netzwerkkonnektivität (optional)

Sie können die Konnektivität zwischen Ihrem lokalen Rechenzentrum und Ihrer AWS Infrastruktur mithilfe eines zugehörigen Transit-Gateways oder Direct Connect mithilfe eines AWS Site-to-Site VPN-Anhangs zu einem Transit-Gateway konfigurieren.

Um die Konnektivität zu lokalen Systemen für eine erfolgreiche Bereitstellung der Umgebung zu ermöglichen, müssen Sie die Haupt-Routing-Tabelle der VPC so konfigurieren, dass Datenverkehr zu diesen Systemen zugelassen wird. Weitere Informationen finden Sie unter the section called “Konfigurieren Sie die VPC-Hauptroutentabelle”.

Nachdem die Amazon EVS-Umgebung erstellt wurde, müssen Sie die Transit-Gateway-Routentabellen mit der in der Amazon EVS-Umgebung CIDRs erstellten VPC aktualisieren. Weitere Informationen finden Sie unter the section called “Konfiguration von Transit-Gateway-Routentabellen und Direct Connect-Präfixen für lokale Konnektivität (optional)”.

Weitere Informationen zum Einrichten einer Direct Connect Verbindung finden Sie unter Direct Connect Gateways und Transit-Gateway-Verknüpfungen. Weitere Informationen zur Verwendung von AWS Site-to-Site VPN mit AWS Transit Gateway finden Sie unter AWS Site-to-Site VPN-Anlagen in Amazon VPC Transit Gateways im Amazon VPC Transit Gateway Gateway-Benutzerhandbuch.

> **Note**
>
> Amazon EVS unterstützt keine Konnektivität über eine private virtuelle Schnittstelle (VIF) von AWS Direct Connect oder über eine AWS Site-to-Site VPN-Verbindung, die direkt mit der Underlay-VPC endet.

Richten Sie eine VPC-Route-Server-Instanz mit Endpunkten und Peers ein

Amazon EVS verwendet Amazon VPC Route Server, um BGP-basiertes dynamisches Routing zu Ihrem VPC-Underlay-Netzwerk zu ermöglichen. Sie müssen einen Routenserver angeben, der Routen mit mindestens zwei Route-Server-Endpunkten im Service-Access-Subnetz teilt. Die auf den Route-Server-Peers konfigurierten Peer-ASNs müssen übereinstimmen und die Peer-IP-Adressen müssen eindeutig sein.

Wenn Sie Route Server für HCX-Internetkonnektivität konfigurieren, müssen Sie Route-Server-Propagierungen sowohl für das Dienstzugriffssubnetz als auch für das öffentliche Subnetz konfigurieren, die Sie im ersten Schritt dieses Verfahrens erstellt haben.

Important

Ihre Umgebungsbereitstellung schlägt fehl, wenn Sie die folgenden Amazon EVS-Anforderungen für die VPC Route Server-Konfiguration nicht erfüllen:

- Sie müssen mindestens zwei Route-Server-Endpunkte im Service-Access-Subnetz konfigurieren.
- Bei der Konfiguration des Border Gateway Protocol (BGP) für das Tier-0-Gateway muss der Peer-ASN-Wert des VPC-Routenservers mit dem NSX Edge-Peer-ASN-Wert übereinstimmen.
- Bei der Erstellung der beiden Route-Server-Peers müssen Sie für jeden Endpunkt eine eindeutige IP-Adresse aus dem NSX-Uplink-VLAN verwenden. Diese beiden IP-Adressen werden den NSX Edges während der Bereitstellung der Amazon EVS-Umgebung zugewiesen.
- Wenn Sie die Route-Server-Propagierung aktivieren, müssen Sie sicherstellen, dass alle Routing-Tabellen, die weitergegeben werden, mindestens eine explizite Subnetzzuweisung haben. BGP-Routenankündigung schlägt fehl, wenn weitergegebene Routentabellen keine explizite Subnetzzuweisung haben.

Weitere Informationen zum Einrichten des VPC-Routenservers finden Sie im Tutorial Erste Schritte für Route Server.

Important

Stellen Sie bei der Aktivierung der Route-Server-Propagierung sicher, dass alle Routentabellen, die weitergegeben werden, mindestens eine explizite Subnetzzuweisung haben. Die BGP-Routenankündigung schlägt fehl, wenn die Routentabelle über eine explizite Subnetzzuweisung verfügt.

Note

Für die Erkennung der Route-Server-Peer-Verfügbarkeit unterstützt Amazon EVS nur den standardmäßigen BGP-Keepalive-Mechanismus. Amazon EVS unterstützt keine bidirektionale Multi-Hop-Weiterleitungserkennung (BFD).

> **Note**
>
> Wir empfehlen, persistente Routen für die Route-Server-Instance mit einer dauerhaften Dauer zwischen 1 und 5 Minuten zu aktivieren. Wenn diese Option aktiviert ist, werden Routen in der Routingdatenbank des Routenservers beibehalten, auch wenn alle BGP-Sitzungen enden. Weitere Informationen finden Sie im Amazon VPC Benutzerhandbuch unter Erstellen eines Routenservers.

> **Note**
>
> Wenn Sie ein NAT-Gateway oder ein Transit-Gateway verwenden, stellen Sie sicher, dass Ihr Routenserver korrekt konfiguriert ist, um NSX-Routen an die VPC-Routentabelle (n) weiterzuleiten.

Fehlerbehebung

Wenn Sie auf Probleme stoßen:

- Stellen Sie sicher, dass jede Routing-Tabelle über eine explizite Subnetzzuweisung verfügt.
- Stellen Sie sicher, dass die für den Routenserver und das NSX Tier-0-Gateway eingegebenen Peer-ASN-Werte übereinstimmen.
- Stellen Sie sicher, dass die IP-Adressen der Route-Server-Endpunkte eindeutig sind.
- Überprüfen Sie den Status der Route-Propagierung in Ihren Routentabellen.
- Verwenden Sie die VPC Route Server-Peerprotokollierung, um den Zustand der BGP-Sitzung zu überwachen und Verbindungsprobleme zu beheben. Weitere Informationen finden Sie unter Route-Server-Peer-Logging im Amazon VPC-Benutzerhandbuch.

Erstellen Sie eine Netzwerk-ACL zur Steuerung des Amazon EVS-VLAN-Subnetzverkehrs

Amazon EVS verwendet eine Network Access Control List (ACL), um den Verkehr zu und von Amazon EVS-VLAN-Subnetzen zu steuern. Sie können die Standard-Netzwerk-ACL für Ihre VPC verwenden, oder Sie können eine benutzerdefinierte Netzwerk-ACL für Ihre VPC mit Regeln

erstellen, die den Regeln für Ihre Sicherheitsgruppen ähneln, um Ihrer VPC eine Sicherheitsebene hinzuzufügen. Weitere Informationen finden Sie unter Erstellen einer Netzwerk-ACL für Ihre VPC im Amazon VPC-Benutzerhandbuch.

Wenn Sie beabsichtigen, die HCX-Internetkonnektivität zu konfigurieren, stellen Sie sicher, dass die von Ihnen konfigurierten Netzwerk-ACL-Regeln die erforderlichen eingehenden und ausgehenden Verbindungen für HCX-Komponenten zulassen. Weitere Informationen zu den HCX-Portanforderungen finden Sie im HCX-Benutzerhandbuch. VMware

> **Important**
>
> Wenn Sie eine Verbindung über das Internet herstellen, ermöglicht die Verknüpfung einer Elastic IP-Adresse mit einem VLAN direkten Internetzugriff auf alle Ressourcen in diesem VLAN-Subnetz. Stellen Sie sicher, dass Sie die entsprechenden Listen zur Netzwerkzugriffskontrolle so konfiguriert haben, dass der Zugriff entsprechend Ihren Sicherheitsanforderungen eingeschränkt wird.

> **Important**
>
> EC2-Sicherheitsgruppen funktionieren nicht auf elastischen Netzwerkschnittstellen, die mit Amazon EVS-VLAN-Subnetzen verbunden sind. Um den Verkehr zu und von Amazon EVS VLAN-Subnetzen zu kontrollieren, müssen Sie eine Netzwerkzugriffskontrollliste verwenden.

Erstellen Sie eine Amazon EVS-Umgebung

> **Important**
>
> Um so einfach und schnell wie möglich loszulegen, enthält dieses Thema Schritte zum Erstellen einer Amazon EVS-Umgebung mit Standardeinstellungen. Bevor Sie eine Umgebung erstellen, empfehlen wir Ihnen, sich mit allen Einstellungen vertraut zu machen und eine Umgebung mit den Einstellungen bereitzustellen, die Ihren Anforderungen entsprechen. Umgebungen können nur bei der ersten Umgebungserstellung konfiguriert werden. Umgebungen können nicht geändert werden, nachdem Sie sie erstellt haben. Eine Übersicht über alle möglichen Amazon EVS-Umgebungseinstellungen finden Sie im Amazon EVS API-Referenzhandbuch.

> **Note**
>
> Ihre Umgebungs-ID steht Amazon EVS in allen AWS Regionen zur Verfügung, um die Einhaltung von VCF-Lizenzen zu gewährleisten.

> **Note**
>
> Amazon EVS-Umgebungen müssen in derselben Region und Availability Zone wie die VPC- und VPC-Subnetze bereitgestellt werden.

Führen Sie diesen Schritt aus, um eine Amazon EVS-Umgebung mit Hosts und VLAN-Subnetzen zu erstellen.

Example

Amazon EVS console

1. Gehen Sie zur Amazon EVS-Konsole.

   > **Note**
   >
   > Stellen Sie sicher, dass die AWS Region, die oben rechts auf Ihrer Konsole angezeigt wird, die AWS Region ist, in der Sie Ihre Umgebung erstellen möchten. Ist dies nicht der Fall, wählen Sie das Drop-down-Menü neben dem Namen der AWS Region aus und wählen Sie die AWS Region aus, die Sie verwenden möchten.

2. Wählen Sie im Navigationsbereich Environments (Umgebungen) aus.
3. Wählen Sie Create environment (Umgebung erstellen) aus.
4. Überprüfen Sie auf der Seite „Amazon EVS-Anforderungen validieren“, ob die Serviceanforderungen erfüllt wurden. Weitere Informationen finden Sie unter Amazon Elastic VMware Service einrichten.
   a. (Optional) Geben Sie unter Name einen Umgebungsnamen ein.
   b. Wählen Sie unter Umgebungsversion Ihre VCF-Version aus. Informationen zu den von Amazon EVS bereitgestellten VCF-Versionen finden Sie unter. the section called “VCF-Versionen und EC2-Instances”

c. Geben Sie als Site-ID Ihre Broadcom-Site-ID ein.

d. Geben Sie für VCF-Lösungsschlüssel einen VCF-Lösungsschlüssel ein (VMware vSphere 8 Enterprise Plus for VCF). Dieser Lizenzschlüssel kann nicht von einer vorhandenen Umgebung verwendet werden.

> **Note**
>
> Der VCF-Lösungsschlüssel muss über ausreichend Kerne verfügen. Weitere Informationen finden Sie unter the section called “VCF-Abonnements”.

> **Note**
>
> Ihre VCF-Lizenz steht Amazon EVS in allen AWS Regionen zur Verfügung, um die Einhaltung der Lizenzbestimmungen zu gewährleisten. Amazon EVS validiert keine Lizenzschlüssel. Besuchen Sie den Broadcom-Support, um Lizenzschlüssel zu validieren.

> **Note**
>
> Amazon EVS erfordert, dass Sie einen gültigen VCF-Lösungsschlüssel im SDDC Manager verwalten, damit der Service ordnungsgemäß funktioniert. Wenn Sie den VCF-Lösungsschlüssel nach der Bereitstellung mit dem vSphere Client verwalten, müssen Sie sicherstellen, dass die Schlüssel auch auf dem Lizenzierungsbildschirm der SDDC Manager-Benutzeroberfläche angezeigt werden.

e. Geben Sie für den vSAN-Lizenzschlüssel einen vSAN-Lizenzschlüssel ein. Dieser Lizenzschlüssel kann nicht von einer vorhandenen Umgebung verwendet werden.

> **Note**
>
> Der vSAN-Lizenzschlüssel muss über eine ausreichende vSAN-Kapazität verfügen. Weitere Informationen finden Sie unter the section called “VCF-Abonnements”.

> **Note**
>
> Ihre VCF-Lizenz steht Amazon EVS in allen AWS Regionen zur Verfügung, um die Einhaltung der Lizenzbestimmungen zu gewährleisten. Amazon EVS validiert keine Lizenzschlüssel. Besuchen Sie den Broadcom-Support, um Lizenzschlüssel zu validieren.

> **Note**
>
> Amazon EVS erfordert, dass Sie einen gültigen vSAN-Lizenzschlüssel im SDDC Manager verwalten, damit Sie den Service auswählen können, damit er ordnungsgemäß funktioniert. Wenn Sie den vSAN-Lizenzschlüssel nach der Bereitstellung mit dem vSphere Client verwalten, müssen Sie sicherstellen, dass die Schlüssel auch auf dem Lizenzierungsbildschirm der SDDC Manager-Benutzeroberfläche angezeigt werden.

f. Für die VCF-Lizenzbedingungen klicken Sie das Kästchen an, um zu bestätigen, dass Sie die erforderliche Anzahl an VCF-Softwarelizenzen erworben haben und weiterhin beibehalten werden, um alle physischen Prozessorkerne in der Amazon EVS-Umgebung abzudecken. Informationen zu Ihrer VCF-Software in Amazon EVS werden an Broadcom weitergegeben, um die Einhaltung der Lizenzbestimmungen zu überprüfen.

g. Wählen Sie Weiter aus.

5. Führen Sie auf der Seite „Hostdetails angeben“ die folgenden Schritte viermal aus, um der Umgebung vier Hosts hinzuzufügen. Amazon EVS-Umgebungen benötigen vier Hosts für die erste Bereitstellung.

   a. Wählen Sie Hostdetails hinzufügen aus.

   b. Geben Sie unter DNS-Hostname den Hostnamen für den Host ein.

   c. Wählen Sie als Instance-Typ den EC2-Instance-Typ aus.

   d. Für die ESX-Hostversion wird bei der Erstellung der Umgebung eine ESX-Standardversion für die gewählte VCF-Version verwendet. Weitere Informationen finden Sie unter the section called “VCF-Versionen und EC2-Instances”.

> **Important**
>
> Beenden oder beenden Sie keine EC2-Instances, die Amazon EVS bereitstellt. Diese Aktion führt zu Datenverlust.

e. Wählen Sie für das SSH-Schlüsselpaar ein SSH-Schlüsselpaar für den SSH-Zugriff auf den Host aus.

f. Wählen Sie Host hinzufügen.

6. Gehen Sie auf der Seite Netzwerke und Konnektivität konfigurieren wie folgt vor.

a. Wählen Sie für die HCX-Konnektivitätsanforderungen aus, ob Sie HCX mit privater Konnektivität oder über das Internet verwenden möchten.

b. Wählen Sie für VPC die VPC aus, die Sie zuvor erstellt haben.

c. (Nur für HCX-Internetverbindung) Wählen Sie für HCX-Netzwerk-ACL aus, mit welcher Netzwerk-ACL Ihr HCX-VLAN verknüpft werden soll.

> **Important**
>
> Es wird dringend empfohlen, eine benutzerdefinierte Netzwerk-ACL für das HCX-VLAN zu erstellen. Weitere Informationen finden Sie unter the section called “Netzwerk-ACL konfigurieren”.

d. Wählen Sie für Service Access Subnet das private Subnetz aus, das bei der Erstellung der VPC erstellt wurde.

e. Für Sicherheitsgruppe — optional können Sie bis zu zwei Sicherheitsgruppen auswählen, die die Kommunikation zwischen der Amazon EVS-Steuerebene und der VPC steuern. Amazon EVS verwendet die Standardsicherheitsgruppe, wenn keine Sicherheitsgruppe ausgewählt wurde.

> **Note**
>
> Stellen Sie sicher, dass die von Ihnen ausgewählten Sicherheitsgruppen Konnektivität zu Ihren DNS-Servern und Amazon EVS-VLAN-Subnetzen bereitstellen.

f. Geben Sie unter Verwaltungskonnektivität die CIDR-Blöcke ein, die für die Amazon EVS-VLAN-Subnetze verwendet werden sollen. Wenn Sie für den HCX-Uplink-VLAN-CIDR-

Block ein öffentliches HCX-VLAN konfigurieren, müssen Sie einen CIDR-Block mit einer Netzmaskenlänge von genau /28 angeben. Amazon EVS gibt einen Validierungsfehler aus, wenn eine andere CIDR-Blockgröße für das öffentliche HCX-VLAN angegeben ist. Für ein privates HCX-VLAN und alle anderen VLANs CIDR-Blöcke ist die minimale Netzmaskenlänge, die Sie verwenden können, /28 und die Höchstlänge /24.

> **Important**
>
> Amazon EVS-VLAN-Subnetze können nur während der Erstellung der Amazon EVS-Umgebung erstellt werden und können nach der Erstellung der Umgebung nicht geändert werden. Sie müssen sicherstellen, dass die CIDR-Blöcke des VLAN-Subnetzes die richtige Größe haben, bevor Sie die Umgebung erstellen. Nach der Bereitstellung der Umgebung können Sie keine VLAN-Subnetze hinzufügen. Weitere Informationen finden Sie unter the section called “Überlegungen zum Amazon EVS-Netzwerk”.

g. Geben Sie unter Erweiterung VLANs die CIDR-Blöcke für zusätzliche Amazon EVS-VLAN-Subnetze ein, die zur Erweiterung der VCF-Funktionen innerhalb von Amazon EVS verwendet werden können, z. B. zur Aktivierung von NSX Federation.

h. Geben Sie unter Workload/VCF-Konnektivität den CIDR-Block für das NSX-Uplink-VLAN ein und wählen Sie zwei VPC-Route-Server-Peer aus, IDs die über den NSX-Uplink zu Route Server-Endpunkten führen.

> **Note**
>
> Amazon EVS benötigt vor der EVS-Bereitstellung eine VPC-Route-Server-Instance, die zwei Route Server-Endpunkten und zwei Route Server-Peers zugeordnet ist. Diese Konfiguration ermöglicht dynamisches BGP-basiertes Routing über den NSX-Uplink. Weitere Informationen finden Sie unter the section called “Richten Sie eine VPC-Route-Server-Instanz mit Endpunkten und Peers ein”.

i. Wählen Sie Weiter aus.

7. Gehen Sie auf der Seite „Management-DNS-Hostnamen angeben“ wie folgt vor.

   a. Geben Sie unter DNS-Hostnamen der Verwaltungs-Appliance die DNS-Hostnamen für die virtuellen Maschinen ein, auf denen VCF-Verwaltungs-Appliances gehostet werden sollen. Wenn Sie Route 53 als DNS-Anbieter verwenden, wählen Sie auch die gehostete Zone aus, die Ihre DNS-Einträge enthält.

b. Wählen Sie unter Anmeldeinformationen aus, ob Sie den AWS verwalteten KMS-Schlüssel für Secrets Manager oder einen von Ihnen bereitgestellten vom Kunden verwalteten KMS-Schlüssel verwenden möchten. Dieser Schlüssel wird verwendet, um die VCF-Anmeldeinformationen zu verschlüsseln, die für die Verwendung von SDDC Manager, NSX Manager und vCenter Appliances erforderlich sind.

> **Note**
>
> Im Zusammenhang mit vom Kunden verwalteten KMS-Schlüsseln fallen Nutzungskosten an. Weitere Informationen finden Sie auf der Seite mit den AWS KMS-Preisen.

c. Wählen Sie Weiter aus.

8. (Optional) Fügen Sie auf der Seite „Tags hinzufügen“ alle Tags hinzu, die dieser Umgebung zugewiesen werden sollen, und wählen Sie Weiter aus.

> **Note**
>
> Hosts, die als Teil dieser Umgebung erstellt wurden, erhalten das folgende Tag:`DoNotDelete-EVS-<environmentid>-<hostname>`.

> **Note**
>
> Tags, die der Amazon EVS-Umgebung zugeordnet sind, werden nicht auf zugrunde liegende AWS Ressourcen wie EC2-Instances übertragen. Sie können Tags für zugrunde liegende AWS Ressourcen mithilfe der jeweiligen Servicekonsole oder der erstellen. AWS CLI

9. Überprüfen Sie auf der Seite Überprüfen und erstellen Ihre Konfiguration und wählen Sie Umgebung erstellen aus.

> **Important**
>
> Während der Bereitstellung der Umgebung erstellt Amazon EVS die EVS-VLAN-Subnetze und ordnet sie implizit der Haupt-Routing-Tabelle zu. Nach Abschluss der Bereitstellung müssen Sie die Amazon EVS-VLAN-Subnetze explizit einer

Routentabelle für NSX-Konnektivitätszwecke zuordnen. Weitere Informationen finden Sie unter the section called “Ordnen Sie Amazon EVS-VLAN-Subnetze explizit einer VPC-Routentabelle zu”.

> **Note**
>
> Amazon EVS stellt eine aktuelle gebündelte Version von VMware Cloud Foundation bereit, die möglicherweise keine einzelnen Produktupdates, sogenannte asynchrone Patches, enthält. Nach Abschluss dieser Bereitstellung empfehlen wir Ihnen dringend, einzelne Produkte mit dem Async Patch Tool (AP Tool) von Broadcom oder dem im Produkt integrierten LCM-Automatisierung SDDC Manager zu überprüfen und zu aktualisieren. NSX-Upgrades müssen außerhalb von SDDC Manager durchgeführt werden.

> **Note**
>
> Die Erstellung der Umgebung kann mehrere Stunden dauern.

AWS CLI

1. Öffnen Sie eine Terminalsitzung.
2. Erstellen Sie eine Amazon EVS-Umgebung. Im Folgenden finden Sie eine `aws evs create-environment` Musteranfrage.

> **Important**
>
> Bevor Sie den `aws evs create-environment` Befehl ausführen, überprüfen Sie, ob alle Amazon EVS-Voraussetzungen erfüllt sind. Die Bereitstellung der Umgebung schlägt fehl, wenn die Voraussetzungen nicht erfüllt sind. Weitere Informationen finden Sie unter Amazon Elastic VMware Service einrichten.

> **Important**
>
> Während der Bereitstellung der Umgebung erstellt Amazon EVS die EVS-VLAN-Subnetze und ordnet sie implizit der Haupt-Routing-Tabelle zu. Nach Abschluss der Bereitstellung müssen Sie die Amazon EVS-VLAN-Subnetze explizit einer Routentabelle für NSX-Konnektivitätszwecke zuordnen. Weitere Informationen finden Sie unter the section called “Ordnen Sie Amazon EVS-VLAN-Subnetze explizit einer VPC-Routentabelle zu”.

> **Note**
>
> Amazon EVS stellt eine aktuelle gebündelte Version von VMware Cloud Foundation bereit, die möglicherweise keine einzelnen Produktupdates, sogenannte asynchrone Patches, enthält. Nach Abschluss dieser Bereitstellung empfehlen wir Ihnen dringend, einzelne Produkte mithilfe des Async Patch Tool (AP Tool) von Broadcom oder der produktinternen LCM-Automatisierung SDDC Manager zu überprüfen und zu aktualisieren. NSX-Upgrades müssen außerhalb von SDDC Manager durchgeführt werden.

> **Note**
>
> Die Bereitstellung der Umgebung kann mehrere Stunden dauern.

- Geben Sie für die VPC an`--vpc-id`, die Sie zuvor mit einem IPv4 CIDR-Mindestbereich von /22 erstellt haben.
- Geben Sie für `--service-access-subnet-id` die eindeutige ID des privaten Subnetzes an, das bei der Erstellung der VPC erstellt wurde.
- Weitere Informationen finden Sie unter the section called “VCF-Versionen und EC2-Instances” VCF-Versionen`--vcf-version`, die von Amazon EVS bereitgestellt werden,
- Mit bestätigen Sie`--terms-accepted`, dass Sie die erforderliche Anzahl von VCF-Softwarelizenzen erworben haben und weiterhin beibehalten werden, um alle physischen Prozessorkerne in der Amazon EVS-Umgebung abzudecken. Informationen zu Ihrer VCF-

Software in Amazon EVS werden an Broadcom weitergegeben, um die Einhaltung der Lizenzbestimmungen zu überprüfen.

- Geben Sie für `--license-info` Ihren VCF-Lösungsschlüssel (VMware vSphere 8 Enterprise Plus für VCF) und Ihren vSAN-Lizenzschlüssel ein.

> **Note**
>
> Die Anforderungen für den VCF-Lösungsschlüssel (einschließlich der Mindestanzahl an Kernen) und den vSAN-Lizenzschlüssel (einschließlich vSAN-Mindestkapazität) variieren je nach Instanztyp. Spezifische Schwellenwerte für Ihre Konfiguration finden Sie unter. the section called “VCF-Abonnements”

> **Note**
>
> Amazon EVS erfordert, dass Sie einen gültigen VCF-Lösungsschlüssel und einen gültigen vSAN-Lizenzschlüssel im SDDC Manager verwalten, damit der Service ordnungsgemäß funktioniert. Wenn Sie diese Lizenzschlüssel nach der Bereitstellung mit dem vSphere Client verwalten, müssen Sie sicherstellen, dass sie auch im Lizenzierungsbildschirm der SDDC Manager-Benutzeroberfläche angezeigt werden.

> **Note**
>
> Der VCF-Lösungsschlüssel und der vSAN-Lizenzschlüssel können nicht von einer vorhandenen Amazon EVS-Umgebung verwendet werden.

- `--initial-vlans`Geben Sie nämlich die CIDR-Bereiche für die Amazon EVS-VLAN-Subnetze an, die Amazon EVS in Ihrem Namen erstellt. Diese VLANs werden zur Bereitstellung von VCF-Management-Appliances verwendet. Wenn Sie ein öffentliches HCX-VLAN konfigurieren, müssen Sie einen CIDR-Block mit einer Netzmaskenlänge von genau /28 angeben. Amazon EVS gibt einen Validierungsfehler aus, wenn eine andere CIDR-Blockgröße für das öffentliche HCX-VLAN angegeben ist. Für ein privates HCX-VLAN und alle anderen VLANs CIDR-Blöcke ist die minimale Netzmaskenlänge, die Sie verwenden können, /28 und die Höchstlänge /24.
- `hcxNetworkAclId`wird bei der Konfiguration der HCX-Internetkonnektivität verwendet. Geben Sie eine benutzerdefinierte Netzwerk-ACL für das öffentliche HCX-VLAN an.

> **Important**
>
> Es wird dringend empfohlen, eine benutzerdefinierte Netzwerk-ACL für das HCX-VLAN zu erstellen. Weitere Informationen finden Sie unter the section called “Netzwerk-ACL konfigurieren”.

> **Important**
>
> Amazon EVS-VLAN-Subnetze können nur während der Erstellung der Amazon EVS-Umgebung erstellt werden und können nach der Erstellung der Umgebung nicht geändert werden. Sie müssen sicherstellen, dass die CIDR-Blöcke des VLAN-Subnetzes die richtige Größe haben, bevor Sie die Umgebung erstellen. Nach der Bereitstellung der Umgebung können Sie keine VLAN-Subnetze hinzufügen. Weitere Informationen finden Sie unter the section called “Überlegungen zum Amazon EVS-Netzwerk”.

- Geben Sie für `--hosts` Hostdetails für die Hosts an, die Amazon EVS für die Bereitstellung der Umgebung benötigt. Geben Sie für jeden Host den DNS-Hostnamen, den EC2-SSH-Schlüsselnamen und den EC2-Instance-Typ an. Die dedizierte Host-ID ist optional.

> **Important**
>
> Beenden oder beenden Sie keine EC2-Instances, die Amazon EVS bereitstellt. Diese Aktion führt zu Datenverlust.

- Geben Sie für `--connectivity-info` den 2-VPC-Routenserver-Peer an IDs , den Sie im vorherigen Schritt erstellt haben.

> **Note**
>
> Amazon EVS benötigt vor der EVS-Bereitstellung eine VPC-Route-Server-Instance, die zwei Route Server-Endpunkten und zwei Route Server-Peers zugeordnet ist. Diese Konfiguration ermöglicht dynamisches BGP-basiertes Routing über den NSX-Uplink. Weitere Informationen finden Sie unter the section called “Richten Sie eine VPC-Route-Server-Instanz mit Endpunkten und Peers ein”.

- Geben Sie für die DNS-Hostnamen für die virtuellen Maschinen ein`--vcf-hostnames`, auf denen VCF-Verwaltungs-Appliances gehostet werden sollen.
- Geben Sie für `--site-id` Ihre eindeutige Broadcom-Site-ID ein. Diese ID ermöglicht den Zugriff auf das Broadcom-Portal und wird Ihnen von Broadcom bei Abschluss oder Verlängerung Ihres Softwarevertrags zur Verfügung gestellt.
- (Optional) Geben Sie für `--region` die Region ein, in der Ihre Umgebung bereitgestellt werden soll. Wenn die Region nicht angegeben ist, wird Ihre Standardregion verwendet.

```
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
```

Im Folgenden wird eine Beispielantwort dargestellt:

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

Überprüfen Sie die Erstellung der Amazon EVS-Umgebung

Example

Amazon EVS console

1. Gehen Sie zur Amazon EVS-Konsole.
2. Wählen Sie im Navigationsbereich Environments (Umgebungen) aus.
3. Wählen Sie die Umgebung aus.
4. Wählen Sie die Registerkarte Details aus.
5. Vergewissern Sie sich, dass der Umgebungsstatus „Überstanden“ und der Umgebungsstatus „Erstellt“ lautet. Dadurch wissen Sie, dass die Umgebung einsatzbereit ist.

> **Note**
>
> Die Erstellung der Umgebung kann mehrere Stunden dauern. Wenn im Umgebungsstatus immer noch Creating angezeigt wird, aktualisieren Sie die Seite.

AWS CLI

1. Öffnen Sie eine Terminalsitzung.
2. Führen Sie den folgenden Befehl aus und verwenden Sie dabei die Umgebungs-ID für Ihre Umgebung und den Namen der Region, die Ihre Ressourcen enthält. Die Umgebung ist einsatzbereit, wenn dies der Fall `environmentState` ist`CREATED`.

> **Note**
>
> Die Erstellung der Umgebung kann mehrere Stunden dauern. Wenn das `environmentState` immer noch angezeigt wird`CREATING`, führen Sie den Befehl erneut aus, um die Ausgabe zu aktualisieren.

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

Im Folgenden wird eine Beispielantwort dargestellt:

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

Ordnen Sie Amazon EVS-VLAN-Subnetze explizit einer VPC-Routentabelle zu

Ordnen Sie jedes der Amazon EVS-VLAN-Subnetze explizit einer Routing-Tabelle in Ihrer VPC zu. Diese Routing-Tabelle wird verwendet, um AWS Ressourcen die Kommunikation mit virtuellen Maschinen in NSX-Netzwerksegmenten zu ermöglichen, die mit Amazon EVS ausgeführt werden. Wenn Sie ein öffentliches HCX-VLAN erstellt haben, stellen Sie sicher, dass Sie das öffentliche HCX-VLAN-Subnetz explizit einer öffentlichen Routentabelle in Ihrer VPC zuordnen, die zu einem Internet-Gateway weiterleitet.

Example

Amazon VPC console

1. Gehen Sie zur VPC-Konsole.
2. Wählen Sie im Navigationsbereich Route Tables (Routing-Tabellen) aus.
3. Wählen Sie die Routing-Tabelle aus, die Sie Amazon EVS-VLAN-Subnetzen zuordnen möchten.
4. Wählen Sie die Registerkarte Subnetzzuordnungen aus.
5. Wählen Sie unter Explizite Subnetzzuordnungen die Option Subnetzzuordnungen bearbeiten aus.
6. Wählen Sie alle Amazon EVS-VLAN-Subnetze aus.
7. Klicken Sie auf Save associations (Zuordnungen speichern).

AWS CLI

1. Öffnen Sie eine Terminalsitzung.
2. Identifizieren Sie das Amazon EVS-VLAN-Subnetz. IDs

```
aws ec2 describe-subnets
```

3. Ordnen Sie Ihre Amazon EVS-VLAN-Subnetze einer Routing-Tabelle in Ihrer VPC zu.

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

Stellen Sie EIPs eine Verbindung zum öffentlichen HCX-VLAN-Subnetz her (für HCX-Internetkonnektivität)

Gehen Sie wie folgt vor, um die Elastic IP-Adresse (EIPs) aus dem IPAM-Pool dem öffentlichen HCX-VLAN für HCX-Internetkonnektivität zuzuordnen. Sie müssen mindestens zwei Appliances EIPs für die HCX Manager- und HCX Interconnect (HCX-IX) Appliances zuordnen. Ordnen Sie jeder HCX-Netzwerk-Appliance, die Sie bereitstellen müssen, eine zusätzliche EIP zu. Sie können bis zu 13 EIPs aus dem IPAM-Pool haben, die dem öffentlichen HCX-VLAN zugeordnet sind.

Important

Die öffentliche HCX-Internetverbindung schlägt fehl, wenn Sie nicht mindestens zwei EIPs aus dem IPAM-Pool einem öffentlichen HCX-VLAN-Subnetz zuordnen.

Note

Amazon EVS unterstützt derzeit nur die Verbindung EIPs mit dem HCX-VLAN.

Note

Sie können die ersten beiden EIPs oder die letzten EIP aus dem öffentlichen IPAM-CIDR-Block nicht dem VLAN-Subnetz zuordnen. Diese EIPs sind als Netzwerk-, Standard-

Gateway- und Broadcast-Adressen reserviert. Amazon EVS gibt einen Validierungsfehler aus, wenn Sie versuchen, diese EIPs mit dem VLAN-Subnetz zu verknüpfen.

Amazon EVS console

1. Gehen Sie zur Amazon EVS-Konsole.
2. Wählen Sie im Navigationsmenü Umgebungen aus.
3. Wählen Sie die Umgebung aus.
4. Wählen Sie auf der Registerkarte Netzwerke und Konnektivität das öffentliche HCX-VLAN aus.
5. Wählen Sie EIP mit VLAN verknüpfen aus.
6. Wählen Sie die Elastic IP-Adresse (n) aus, die dem öffentlichen HCX-VLAN zugeordnet werden sollen.
7. Wählen Sie Associate EIPs aus.
8. Überprüfen Sie die EIP-Verknüpfungen, um sicherzustellen, dass sie mit dem EIPs öffentlichen HCX-VLAN verknüpft wurden.

AWS CLI

1. Verwenden Sie den Beispielbefehl, um eine Elastic IP-Adresse einem VLAN zuzuordnen. `associate-eip-to-vlan`
   - `environment-id`- Die ID Ihrer Amazon EVS-Umgebung.
   - `vlan-name`— Der Name des VLAN, das der Elastic IP-Adresse zugeordnet werden soll.
   - `allocation-id`— Die Zuweisungs-ID der Elastic IP-Adresse.

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

   Der Befehl gibt Details zum VLAN zurück, einschließlich der neuen EIP-Zuordnung:

   ```
   {
       "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"
    }
}
```


Das `eipAssociations` Array zeigt die neue Assoziation, einschließlich:

- `associationId`- Die eindeutige ID für diese EIP-Assoziation, die für die Trennung der Verbindung verwendet wird.
- `allocationId`— Die Zuweisungs-ID der zugehörigen Elastic IP-Adresse.
- `ipAddress`- Die dem VLAN zugewiesene IP-Adresse.

2. Wiederholen Sie den Schritt, um weitere EIPs Verbindungen herzustellen.

Konfiguration von Transit-Gateway-Routentabellen und Direct Connect-Präfixen für lokale Konnektivität (optional)

Wenn Sie die lokale Netzwerkkonnektivität mithilfe von Direct Connect oder AWS Site-to-Site VPN mit einem Transit-Gateway konfigurieren, müssen Sie die Transit-Gateway-Routentabellen mit der in der Amazon CIDRs EVS-Umgebung erstellten VPC aktualisieren. Weitere Informationen finden Sie unter Transit-Gateway-Routentabellen in Amazon VPC Transit Gateways.

Wenn Sie AWS Direct Connect verwenden, müssen Sie möglicherweise auch Ihre Direct Connect-Präfixe aktualisieren, um aktualisierte Routen von der VPC zu senden und zu empfangen. Weitere Informationen finden Sie unter Erlaubt Präfixinteraktionen für AWS Direct Connect-Gateways.

Rufen Sie VCF-Anmeldeinformationen ab und greifen Sie auf VCF-Verwaltungsgeräte zu

Amazon EVS verwendet AWS Secrets Manager, um verwaltete Geheimnisse in Ihrem Konto zu erstellen, zu verschlüsseln und zu speichern. Diese Geheimnisse enthalten die VCF-Anmeldeinformationen, die für die Installation und den Zugriff auf VCF-Verwaltungs-Appliances wie vCenter Server, NSX und SDDC Manager erforderlich sind, sowie das ESX-Root-Passwort. Weitere Informationen zum Abrufen von Geheimnissen finden Sie unter Geheimnisse aus AWS Secrets Manager abrufen im AWS Secrets Manager Manager-Benutzerhandbuch.

> **Note**
>
> Amazon EVS bietet keine verwaltete Rotation Ihrer Secrets. Wir empfehlen, dass Sie Ihre Secrets regelmäßig in einem bestimmten Rotationsfenster rotieren, um sicherzustellen, dass Secrets nicht zu lange bestehen.

Nachdem Sie Ihre VCF-Anmeldeinformationen von AWS Secrets Manager abgerufen haben, können Sie sie verwenden, um sich bei Ihren VCF-Verwaltungsgeräten anzumelden. Weitere Informationen finden Sie in der Produktdokumentation unter Anmelden bei der SDDC Manager-Benutzeroberfläche und So verwenden und konfigurieren Sie Ihren vSphere Client. VMware

Konfigurieren Sie die serielle EC2-Konsole (optional)

Standardmäßig aktiviert Amazon EVS die ESX Shell auf neu bereitgestellten Amazon EVS-Hosts. Diese Konfiguration ermöglicht den Zugriff auf die serielle Schnittstelle der Amazon EC2 EC2-Instance über die serielle EC2-Konsole, mit der Sie Boot-, Netzwerkkonfigurations- und andere Probleme beheben können. Die serielle Konsole erfordert nicht, dass Ihre Instance über Netzwerkfähigkeiten verfügt. Mit der seriellen Konsole können Sie Befehle für eine laufende EC2-Instance eingeben, als ob Ihre Tastatur und Ihr Monitor direkt an die serielle Schnittstelle der Instance angeschlossen wären.

Auf die serielle EC2-Konsole kann über die EC2-Konsole oder die zugegriffen werden. AWS CLI Weitere Informationen finden Sie unter EC2 Serial Console for Instances im Amazon EC2 EC2-Benutzerhandbuch.

> **Note**
>
> Die serielle EC2-Konsole ist der einzige von Amazon EVS unterstützte Mechanismus für den Zugriff auf die Direct Console User Interface (DCUI), um lokal mit einem ESX-Host zu interagieren.

> **Note**
>
> Amazon EVS deaktiviert standardmäßig Remote-SSH. Weitere Informationen zur Aktivierung von SSH für den Zugriff auf die Remote-ESX Shell finden Sie unter Remote ESX Shell Access with SSH in der VMware vSphere-Produktdokumentation.

Connect zur seriellen EC2-Konsole her

Um eine Verbindung zur seriellen EC2-Konsole herzustellen und das von Ihnen gewählte Tool zur Fehlerbehebung zu verwenden, müssen bestimmte Voraussetzungen erfüllt sein. Weitere Informationen finden Sie unter Voraussetzungen für die serielle EC2-Konsole und Connect zur seriellen EC2-Konsole her im Amazon EC2 EC2-Benutzerhandbuch.

> **Note**
>
> Um eine Verbindung zur seriellen EC2-Konsole herzustellen, muss Ihr EC2-Instance-Status sein. `running` Sie können keine Verbindung zur seriellen Konsole herstellen, wenn sich die Instance im Status`pending`,`stopping`, `stopped`oder `shutting-down` `terminated` befindet. Weitere Informationen zu Änderungen des Instance-Status finden Sie unter Änderung des Amazon EC2 EC2-Instance-Status im Amazon EC2 EC2-Benutzerhandbuch.

Konfigurieren Sie den Zugriff auf die serielle EC2-Konsole

Um den Zugriff auf die serielle EC2-Konsole zu konfigurieren, müssen Sie oder Ihr Administrator den Zugriff auf die serielle Konsole auf Kontoebene gewähren und dann IAM-Richtlinien konfigurieren, um Ihren Benutzern Zugriff zu gewähren. Bei Linux-Instances müssen Sie außerdem auf jeder Instance einen kennwortbasierten Benutzer konfigurieren, damit Ihre Benutzer die serielle Konsole zur Fehlerbehebung verwenden können. Weitere Informationen finden Sie unter Zugriff auf die serielle EC2-Konsole konfigurieren im Amazon EC2 EC2-Benutzerhandbuch.

Bereinigen

Gehen Sie wie folgt vor, um die erstellten AWS Ressourcen zu löschen.

Löschen Sie die Amazon EVS-Hosts und die Umgebung

Gehen Sie wie folgt vor, um die Amazon EVS-Hosts und die Umgebung zu löschen. Diese Aktion löscht die VMware VCF-Installation, die in Ihrer Amazon EVS-Umgebung ausgeführt wird.

> **Note**
>
> Um eine Amazon EVS-Umgebung zu löschen, müssen Sie zuerst alle Hosts in der Umgebung löschen. Eine Umgebung kann nicht gelöscht werden, wenn der Umgebung Hosts zugeordnet sind.

Example

Amazon EVS console

1. Gehen Sie zur Amazon EVS-Konsole.
2. Wählen Sie im Navigationsbereich Umgebung aus.
3. Wählen Sie die Umgebung aus, die die zu löschenden Hosts enthält.
4. Wählen Sie die Registerkarte Hosts aus.
5. Wählen Sie den Host aus und klicken Sie auf der Registerkarte Hosts auf Löschen. Wiederholen Sie diesen Schritt für jeden Host in der Umgebung.
6. Wählen Sie oben auf der Seite Umgebungen die Option Löschen und anschließend Umgebung löschen aus.

   > **Note**
   >
   > Beim Löschen der Umgebung werden auch die Amazon EVS-VLAN-Subnetze und AWS Secrets Manager Manager-Geheimnisse gelöscht, die Amazon EVS erstellt hat. AWS Ressourcen, die Sie erstellen, werden nicht gelöscht. Für diese Ressourcen können weiterhin Kosten anfallen.

7. Wenn Sie Amazon EC2 EC2-Kapazitätsreservierungen eingerichtet haben, die Sie nicht mehr benötigen, stellen Sie sicher, dass Sie diese storniert haben. Weitere Informationen finden Sie unter Stornieren einer Kapazitätsreservierung im Benutzerhandbuch für Amazon EC2.

AWS CLI

1. Öffnen Sie eine Terminalsitzung.
2. Identifizieren Sie die Umgebung, die den zu löschenden Host enthält.

```
aws evs list-environments
```

Im Folgenden wird eine Beispielantwort dargestellt:

```
{
    "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. Löschen Sie die Hosts aus der Umgebung. Im Folgenden finden Sie ein Beispiel für eine `aws evs delete-environment-host` Anfrage.

> **Note**
>
> Um eine Umgebung löschen zu können, müssen Sie zuerst alle Hosts löschen, die in der Umgebung enthalten sind.

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

4. Wiederholen Sie die vorherigen Schritte, um die verbleibenden Hosts in Ihrer Umgebung zu löschen.
5. Löschen Sie die Umgebung.

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

> **Note**
>
> Beim Löschen der Umgebung werden auch die Amazon EVS-VLAN-Subnetze und AWS Secrets Manager Manager-Geheimnisse gelöscht, die Amazon EVS erstellt hat. Andere AWS Ressourcen, die Sie erstellen, werden nicht gelöscht. Für diese Ressourcen können weiterhin Kosten anfallen.

6. Wenn Sie Amazon EC2 EC2-Kapazitätsreservierungen eingerichtet haben, die Sie nicht mehr benötigen, stellen Sie sicher, dass Sie diese storniert haben. Weitere Informationen finden Sie unter Stornieren einer Kapazitätsreservierung im Benutzerhandbuch für Amazon EC2.

IPAM-Ressourcen löschen (für HCX-Internetkonnektivität)

Wenn Sie die HCX-Internetverbindung konfiguriert haben, gehen Sie wie folgt vor, um Ihre IPAM-Ressourcen zu löschen.

1. Geben Sie EIP-Zuweisungen aus dem öffentlichen IPAM-Pool frei. Weitere Informationen finden Sie unter Freigabe einer Zuweisung im VPC IP Address Manager-Benutzerhandbuch.

2. Entfernen Sie die Bereitstellung des öffentlichen IPv4 CIDR aus dem IPAM-Pool. Weitere Informationen finden Sie unter Deprovision CIDRs aus einem Pool im VPC IP Address Manager-Benutzerhandbuch.
3. Löschen Sie den öffentlichen IPAM-Pool. Weitere Informationen finden Sie unter Löschen eines Pools im VPC IP Address Manager-Benutzerhandbuch.
4. Löschen Sie das IPAM. Weitere Informationen finden Sie unter Löschen eines IPAM im VPC IP Address Manager-Benutzerhandbuch.

Löschen Sie die VPC-Routenserver-Komponenten

Schritte zum Löschen der von Ihnen erstellten Amazon VPC Route Server-Komponenten finden Sie unter Route Server Cleanup im Amazon VPC-Benutzerhandbuch.

Löschen Sie die Network Access Control List (ACL)

Schritte zum Löschen einer Netzwerkzugriffskontrollliste finden Sie unter Löschen einer Netzwerk-ACL für Ihre VPC im Amazon VPC-Benutzerhandbuch.

Trennen Sie die Zuordnung und löschen Sie die Subnetz-Routentabellen

Schritte zum Trennen und Löschen von Subnetz-Routentabellen finden Sie unter Subnetz-Routentabellen im Amazon VPC-Benutzerhandbuch.

Subnetze löschen

Löschen Sie die VPC-Subnetze, einschließlich des Dienstzugriffssubnetzes. Schritte zum Löschen von VPC-Subnetzen finden Sie unter Löschen eines Subnetzes im Amazon VPC-Benutzerhandbuch.

> **Note**
>
> Wenn Sie Route 53 für DNS verwenden, entfernen Sie die eingehenden Endpunkte, bevor Sie versuchen, das Dienstzugriffssubnetz zu löschen. Andernfalls können Sie das Dienstzugriffssubnetz nicht löschen.

> **Note**
>
> Amazon EVS löscht die VLAN-Subnetze in Ihrem Namen, wenn die Umgebung gelöscht wird. Amazon EVS VLAN-Subnetze können nur gelöscht werden, wenn die Umgebung gelöscht wird.

Löschen der VPC

Schritte zum Löschen der VPC finden Sie unter Löschen Ihrer VPC im Amazon VPC-Benutzerhandbuch.

Nächste Schritte

Migrieren Sie Ihre Workloads mithilfe der VMware Hybrid Cloud Extension (VMware HCX) zu Amazon EVS. Weitere Informationen finden Sie unter Migration.

Migrieren Sie Workloads mit HCX zu Amazon EVS VMware

Nach der Bereitstellung von Amazon EVS können Sie VMware HCX mit privater oder öffentlicher Internetverbindung bereitstellen, um die Migration von Workloads zu Amazon EVS zu erleichtern. Weitere Informationen finden Sie unter Erste Schritte mit VMware HCX im HCX-Benutzerhandbuch.

VMware

> **Important**
>
> Die internetbasierte HCX-Migration wird im Allgemeinen nicht empfohlen für:
>
> - Anwendungen, die empfindlich auf Netzwerkjitter oder Latenz reagieren.
> - Zeitkritische vMotion-Operationen.
> - Umfangreiche Migrationen mit strengen Leistungsanforderungen.
>
> Für diese Szenarien empfehlen wir die Verwendung von HCX Private Connectivity. Eine private, dedizierte Verbindung bietet im Vergleich zu internetbasierten Verbindungen eine zuverlässigere Leistung.

HCX-Konnektivitätsoptionen

Sie können Workloads über private Konnektivität mit AWS Direct Connect oder Site-to-Site VPN-Verbindung oder über öffentliche Konnektivität zu Amazon EVS migrieren.

Abhängig von Ihrer Situation und Ihren Verbindungsoptionen bevorzugen Sie möglicherweise die öffentliche oder private Konnektivität mit HCX. Beispielsweise verfügen einige Standorte möglicherweise über private Konnektivität mit höherer Leistungskonstanz, aber geringerem Durchsatz aufgrund von VPN-Verschlüsselung oder begrenzten Verbindungsgeschwindigkeiten. Ebenso verfügen Sie möglicherweise über eine öffentliche Internetverbindung mit hohem Durchsatz, bei der die Leistung stärker schwankt. Mit Amazon EVS haben Sie die Wahl, die Verbindungsoption zu verwenden, die für Sie am besten geeignet ist.

In der folgenden Tabelle werden die Unterschiede zwischen privater und öffentlicher HCX-Konnektivität verglichen.

Private Konnektivität	Öffentliche Konnektivität
Übersicht	Übersicht
Verwendet nur private Verbindungen innerhalb der VPC. Sie können optional AWS Direct Connect oder Site-to-Site VPN mit einem Transit-Gateway für externe Netzwerkk onnektivität verwenden.	Nutzt öffentliche Internetkonnektivität mit Elastic IP-Adressen und ermöglicht so Migrationen ohne eigene private Verbindung.
Am besten geeignet für	Am besten geeignet für
• Zeitkritische vMotion-Operationen. • Umfangreiche Migrationen. • Anwendungen, die empfindlich auf Latenz/Jitter reagieren. • Datenübertragungen mit hohem Datenvolumen. • Organizations mit vorhandenem AWS Direct Connect/VPN AWS Site-to-Site .	• Standorte ohne AWS Direct Connect/VPN AWS Site-to-Site . • Kostensensible Projekte.
Die wichtigsten Vorteile	Die wichtigsten Vorteile
• Konsistente Konnektivität mit niedriger Latenz. • Dedizierte Bandbreitenzuweisung. • Zuverlässigere Netzwerkleistung. • Die standardmäßige HCX-Verschlüsselung kann für private Umgebungen deaktiviert werden, um die Leistung zu optimieren. • Kein öffentliches IP-Management erforderlich.	• Schnellere Einrichtung als private Konnektivität. • Kostengünstig für kleinere Migrationen.
Die wichtigsten Überlegungen	Die wichtigsten Überlegungen
• Komplexere Ersteinrichtung.	• Variablere Netzwerkleistung.

Private Konnektivität	Öffentliche Konnektivität
• Höhere Infrastrukturkosten im Voraus. • Längerer Implementierungszeitraum. • Keine direkte Internetverbindung für eine HCX-Komponente.	• Bandbreitenbeschränkungen sind möglich. • Höhere Latenz als bei privater Konnektivität. • Jede Komponente benötigt eine dedizierte Elastic IP-Adresse, die aus dem öffentlichen IPAM-Pool zugewiesen wird. • EIP-Zuordnungen ermöglichen eine direkte Internetverbindung für jede HCX-Kompo nente.

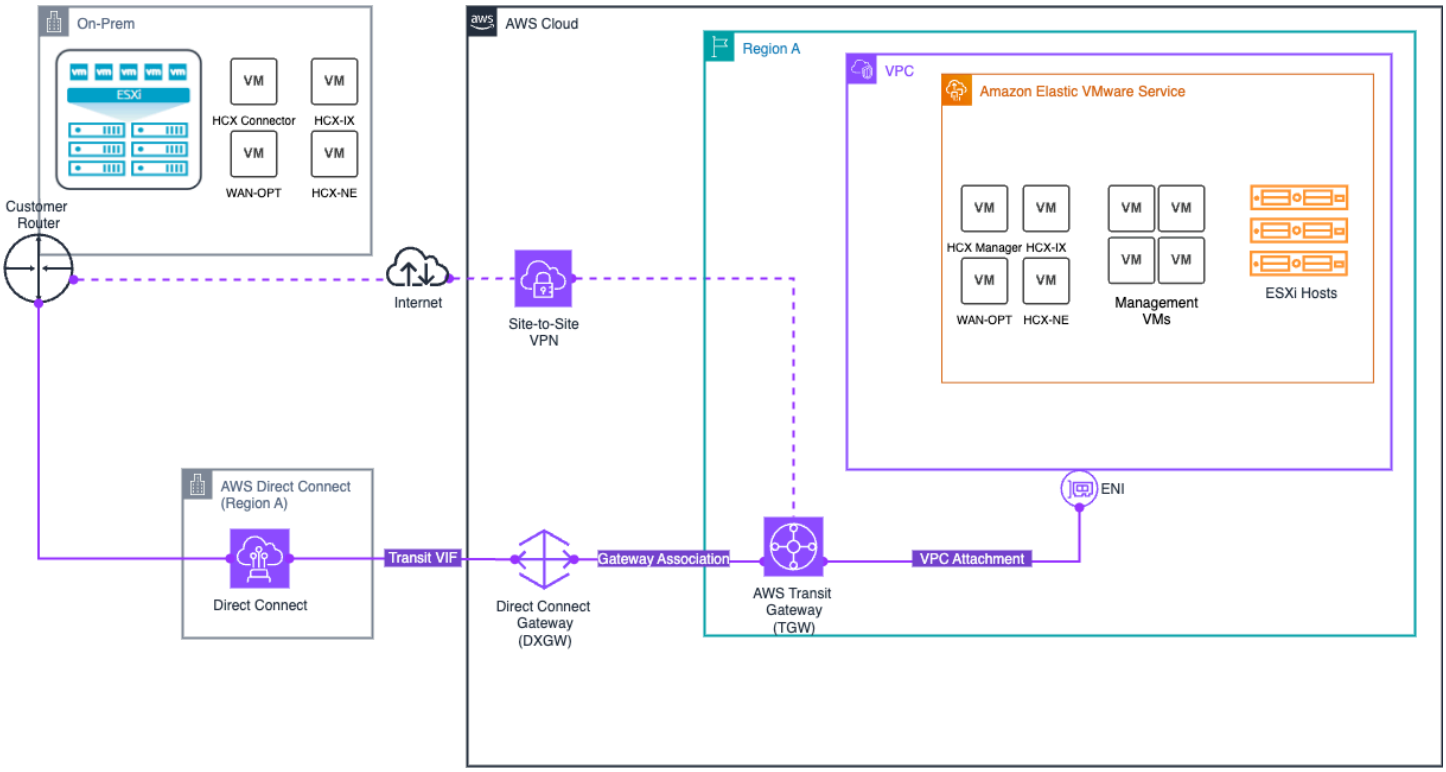
Private HCX-Konnektivitätsarchitektur

Die private HCX-Konnektivitätslösung integriert mehrere Komponenten:

- Amazon EVS-Netzwerkkomponenten
  - Verwendet nur private VLAN-Subnetze für die sichere Kommunikation, einschließlich eines privaten HCX-VLAN.
  - Unterstützt das Netzwerk ACLs zur Verkehrskontrolle.
  - Unterstützt die dynamische BGP-Weitergabe von Routen über einen privaten VPC-Routenserver.
- AWS verwaltete Netzwerk-Transitoptionen für lokale Konnektivität
  - AWS Direct Connect + AWS Transit Gateway ermöglicht es Ihnen, Ihr lokales Netzwerk über eine private, dedizierte Verbindung mit Amazon EVS zu verbinden. Weitere Informationen finden Sie unter AWS Direct Connect + AWS Transit Gateway.
  - AWS Site-to-Site VPN + AWS Transit Gateway bietet die Möglichkeit, eine IPsec VPN-Verbindung zwischen Ihrem Remote-Netzwerk und dem Transit-Gateway über das Internet herzustellen. Weitere Informationen finden Sie unter AWS Transit Gateway + AWS Site-to-Site VPN.

> **Note**
>
> Amazon EVS unterstützt keine Konnektivität über eine private virtuelle Schnittstelle (VIF) von AWS Direct Connect oder über eine AWS Site-to-Site VPN-Verbindung, die direkt mit der Underlay-VPC endet.

Das folgende Diagramm veranschaulicht die private HCX-Konnektivitätsarchitektur und zeigt, wie Sie AWS Direct Connect und Site-to-Site VPN mit dem Transit-Gateway verwenden können, um eine sichere Workload-Migration über eine private, dedizierte Verbindung zu ermöglichen.



HCX-Architektur für Internetkonnektivität

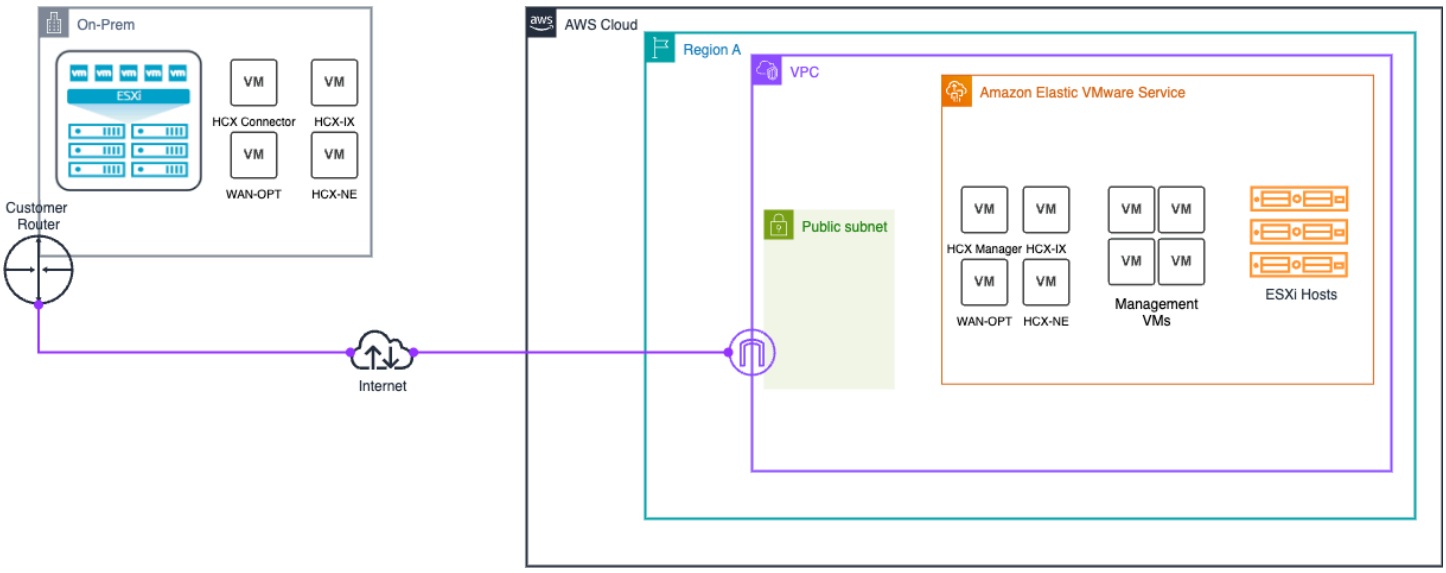
Die HCX-Internetverbindungslösung besteht aus mehreren Komponenten, die zusammenarbeiten:

- Amazon EVS-Netzwerkkomponenten
  - Verwendet ein isoliertes öffentliches HCX-VLAN-Subnetz, um die Internetverbindung zwischen Amazon EVS und Ihren lokalen HCX-Appliances zu ermöglichen.
  - ACLs Unterstützt das Netzwerk zur Datenverkehrskontrolle.

  - Unterstützt die dynamische BGP-Weitergabe von Routen über einen öffentlichen VPC-Routenserver.
- IPAM und öffentliches IP-Management
  - Amazon VPC IP Address Manager (IPAM) verwaltet die Zuweisung öffentlicher IPv4 Adressen aus dem öffentlichen IPAM-Pool von Amazon.
  - Der sekundäre VPC-CIDR-Block (/28) wird aus dem IPAM-Pool zugewiesen, wodurch ein isoliertes öffentliches Subnetz entsteht, das vom Haupt-VPC-CIDR getrennt ist.

Weitere Informationen finden Sie unter the section called “Öffentliche HCX-Konnektivität”.

Das folgende Diagramm veranschaulicht die HCX-Internetkonnektivitätsarchitektur.



Einrichtung der HCX-Migration

In diesem Tutorial wird beschrieben, wie Sie VMware HCX für die Migration Ihrer Workloads zu Amazon EVS konfigurieren.

Voraussetzungen

Stellen Sie vor der Verwendung von VMware HCX mit Amazon EVS sicher, dass die HCX-Voraussetzungen erfüllt sind. Weitere Informationen finden Sie unter the section called “VMware HCX-Voraussetzungen”.

Important

Amazon EVS hat besondere Anforderungen an die öffentliche HCX-Internetkonnektivität. Wenn Sie öffentliche HCX-Konnektivität benötigen, müssen Sie die folgenden Anforderungen erfüllen:

- Erstellen Sie einen IPAM und einen öffentlichen IPv4 IPAM-Pool mit CIDR, die eine Mindestnetzmaskenlänge von /28 haben.
- Weisen Sie den HCX Manager- und HCX Interconnect (HCX-IXEIPs) -Appliances mindestens zwei Elastic IP-Adressen () aus dem IPAM-Pool zu. Weisen Sie jeder HCX-Netzwerk-Appliance, die Sie bereitstellen müssen, eine zusätzliche Elastic IP-Adresse zu.
- Fügen Sie den öffentlichen IPv4 CIDR-Block als zusätzlichen CIDR zu Ihrer VPC hinzu.

Weitere Informationen finden Sie unter the section called “Einrichtung der HCX-Internetverbindung”.

Überprüfen Sie den Status des HCX-VLAN-Subnetzes

Ein VLAN wird für HCX als Teil der standardmäßigen Amazon EVS-Bereitstellung erstellt. Gehen Sie wie folgt vor, um zu überprüfen, ob das HCX-VLAN-Subnetz ordnungsgemäß konfiguriert ist.

Example

Amazon EVS console

1. Gehen Sie zur Amazon EVS-Konsole.
2. Wählen Sie im Navigationsbereich Environments (Umgebungen) aus.
3. Wählen Sie die Amazon EVS-Umgebung aus.
4. Wählen Sie die Registerkarte Netzwerke und Konnektivität aus.
5. Identifizieren Sie unter VLANsdas HCX-VLAN und überprüfen Sie, ob der Status „Erstellt“ und „Öffentlich“ wahr ist.

AWS CLI

1. Führen Sie den folgenden Befehl aus und verwenden Sie dabei die Umgebungs-ID für Ihre Umgebung und den Namen der Region, die Ihre Ressourcen enthält.

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

2. Identifizieren Sie in der Antwortausgabe das VLAN mit einem `functionName` of `hcx` und überprüfen Sie, ob das aktiviert `vlanState` ist `CREATED` und auf `true` gesetzt `isPublic` ist. Im Folgenden wird eine Beispielantwort dargestellt:


```
{
    "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
        }
    ]
}
```

Vergewissern Sie sich, dass das HCX-VLAN-Subnetz einer Netzwerk-ACL zugeordnet ist

Gehen Sie wie folgt vor, um zu überprüfen, ob das HCX-VLAN-Subnetz einer Netzwerk-ACL zugeordnet ist. Weitere Informationen zur Netzwerk-ACL-Zuordnung finden Sie unter. the section called “Erstellen Sie eine Netzwerk-ACL zur Steuerung des Amazon EVS-VLAN-Subnetzverkehrs”

> **Important**
>
> Wenn Sie eine Verbindung über das Internet herstellen, ermöglicht die Verknüpfung einer Elastic IP-Adresse mit einem VLAN direkten Internetzugriff auf alle Ressourcen in diesem VLAN. Stellen Sie sicher, dass Sie die entsprechenden Listen zur Netzwerkzugriffskontrolle so konfiguriert haben, dass der Zugriff entsprechend Ihren Sicherheitsanforderungen eingeschränkt wird.

> **Important**
>
> EC2 Sicherheitsgruppen funktionieren nicht auf elastischen Netzwerkschnittstellen, die mit Amazon EVS-VLAN-Subnetzen verbunden sind. Um den Verkehr zu und von Amazon EVS VLAN-Subnetzen zu kontrollieren, müssen Sie eine Network Access Control List (ACL) verwenden.

Example

Amazon VPC console

1. Gehen Sie zur Konsole. Amazon VPC
2. Wählen Sie im Navigationsbereich Netzwerk aus ACLs.
3. Wählen Sie die Netzwerk-ACL aus, der Ihre VLAN-Subnetze zugeordnet sind.
4. Wählen Sie die Registerkarte Subnetzzuordnungen aus.

5. Vergewissern Sie sich, dass das HCX-VLAN-Subnetz unter den zugehörigen Subnetzen aufgeführt ist.

AWS CLI

1. Führen Sie den folgenden Befehl aus und verwenden Sie dabei die HCX-VLAN-Subnetz-ID im Filter. `Values`

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

2. Vergewissern Sie sich, dass in der Antwort die richtige Netzwerk-ACL zurückgegeben wird.

Stellen Sie sicher, dass EVS-VLAN-Subnetze explizit einer Routing-Tabelle zugeordnet sind

Amazon EVS erfordert, dass alle EVS-VLAN-Subnetze explizit einer Routing-Tabelle in Ihrer VPC zugeordnet werden. Für HCX-Internetkonnektivität muss Ihr öffentliches HCX-VLAN-Subnetz explizit mit einer öffentlichen Routing-Tabelle in Ihrer VPC verknüpft werden, die zu einem Internet-Gateway weiterleitet. Gehen Sie wie folgt vor, um die explizite Zuordnung der Routentabelle zu überprüfen.

Example

Amazon VPC console

1. Gehen Sie zur VPC-Konsole.
2. Wählen Sie im Navigationsbereich Route Tables (Routing-Tabellen) aus.
3. Wählen Sie die Routentabelle aus, der Ihre EVS-VLAN-Subnetze explizit zugeordnet werden sollen.
4. Wählen Sie die Registerkarte Subnetzzuordnungen aus.
5. Überprüfen Sie unter Explizite Subnetzzuordnungen, ob alle EVS-VLAN-Subnetze aufgeführt sind. Wenn ein VLAN-Subnetz hier nicht aufgeführt ist, ist das VLAN-Subnetz implizit der Haupt-Routing-Tabelle zugeordnet. Damit Amazon EVS ordnungsgemäß funktioniert, müssen Sie alle VLAN-Subnetze explizit einer Routing-Tabelle zuordnen. Für das öffentliche HCX-VLAN-Subnetz benötigen Sie eine zugeordnete öffentliche Routing-Tabelle mit einem Internet-Gateway als Ziel. Um dieses Problem zu beheben, wählen Sie Subnetzzuordnungen bearbeiten und fügen Sie die fehlenden VLAN-Subnetze hinzu.

AWS CLI

1. Öffnen Sie eine Terminalsitzung.
2. Führen Sie den folgenden Beispielbefehl aus, um Details zu all Ihren EVS-VLAN-Subnetzen abzurufen, einschließlich der Zuordnung von Routentabellen. Wenn ein VLAN-Subnetz hier nicht aufgeführt ist, ist das VLAN-Subnetz implizit der Haupt-Routing-Tabelle zugeordnet. Damit Amazon EVS ordnungsgemäß funktioniert, müssen Sie alle VLAN-Subnetze explizit einer Routing-Tabelle zuordnen. Für das öffentliche HCX-VLAN-Subnetz benötigen Sie eine zugeordnete öffentliche Routing-Tabelle mit einem Internet-Gateway als Ziel.

   ```
   aws ec2 describe-subnets
   ```

3. Ordnen Sie Ihre EVS-VLAN-Subnetze explizit einer Routentabelle in Ihrer VPC zu. Im Folgenden finden Sie einen Beispielbefehl.

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

(Für HCX-Internetkonnektivität) Überprüfen Sie, ob sie dem HCX-VLAN-Subnetz zugeordnet EIPs sind

Für jede HCX-Netzwerk-Appliance, die Sie bereitstellen, benötigen Sie eine EIP aus dem IPAM-Pool, die einem öffentlichen HCX-VLAN-Subnetz zugeordnet ist. Sie müssen mindestens zwei EIPs mit dem öffentlichen HCX-VLAN-Subnetz für die HCX Manager- und HCX Interconnect (HCX-IX) -Appliances verknüpfen. Gehen Sie wie folgt vor, um zu überprüfen, ob die erforderlichen EIP-Verknüpfungen vorhanden sind.

> **Important**
>
> Die öffentliche HCX-Internetverbindung schlägt fehl, wenn Sie nicht mindestens zwei EIPs aus dem IPAM-Pool einem öffentlichen HCX-VLAN-Subnetz zuordnen.

> **Note**
>
> Sie können die ersten beiden EIPs oder die letzten EIP aus dem öffentlichen IPAM-CIDR-Block nicht einem VLAN-Subnetz zuordnen. Diese EIPs sind als Netzwerk-, Standard-Gateway- und Broadcast-Adressen reserviert. Amazon EVS gibt einen Validierungsfehler aus, wenn Sie versuchen, diese EIPs mit einem VLAN-Subnetz zu verknüpfen.

Example

Amazon EVS console

1. Gehen Sie zur Amazon EVS-Konsole.
2. Wählen Sie im Navigationsmenü Umgebungen aus.
3. Wählen Sie die Umgebung aus.
4. Wählen Sie auf der Registerkarte Netzwerke und Konnektivität das öffentliche HCX-VLAN aus.
5. Überprüfen Sie auf der Registerkarte EIP-Verknüpfungen, ob sie mit dem EIPs öffentlichen HCX-VLAN verknüpft wurden.

AWS CLI

1. Verwenden Sie den Befehl, um zu überprüfen, EIPs welche dem HCX-VLAN-Subnetz zugeordnet sind. `list-environment-vlans` Verwenden Sie für `environment-id` die eindeutige ID für die EVS-Umgebung, die das HCX-VLAN enthält.

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

   Der Befehl gibt Details zu Ihren VLANs, einschließlich EIP-Zuordnungen, zurück:

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


Das `eipAssociations` Array zeigt die EIP-Assoziation, einschließlich:

- `associationId`- Die eindeutige ID für diese EIP-Zuordnung.
- `allocationId`— Die Zuweisungs-ID der zugehörigen Elastic IP-Adresse.
- `ipAddress`- Die dem VLAN zugewiesene IP-Adresse.

Erstellen Sie eine verteilte Portgruppe mit der öffentlichen HCX-Uplink-VLAN-ID

Gehen Sie zur vSphere Client-Oberfläche und folgen Sie den Schritten unter Hinzufügen einer verteilten Portgruppe, um einem vSphere Distributed Switch eine verteilte Portgruppe hinzuzufügen.

Stellen Sie bei der Konfiguration von Failback innerhalb der vSphere Client-Schnittstelle sicher, dass Uplink1 ein aktiver Uplink und Uplink2 ein Standby-Uplink ist, um Failover zu aktivieren. Active/Standby Geben Sie für die VLAN-Einstellung in der vSphere Client-Schnittstelle die HCX-VLAN-ID ein, die Sie zuvor identifiziert haben.

(Optional) Richten Sie die HCX-WAN-Optimierung ein

> **Note**
>
> Die WAN-Optimierungsfunktion ist in HCX 4.11.3 nicht mehr verfügbar. Weitere Informationen finden Sie in den Versionshinweisen zu HCX 4.11.3.

Der HCX WAN Optimization Service (HCX-WO) verbessert die Leistungsmerkmale von Privatleitungen oder Internetpfaden durch die Anwendung von WAN-Optimierungstechniken wie Datenreduzierung und WAN-Pfadkonditionierung. Der HCX WAN Optimization Service wird für Bereitstellungen empfohlen, die keine 10-Gbit-Pfade für Migrationen reservieren können. In 10-Gbit-Bereitstellungen mit niedriger Latenz führt die Verwendung der WAN-Optimierung möglicherweise nicht zu einer verbesserten Migrationsleistung. Weitere Informationen finden Sie unter Überlegungen und bewährte Methoden zur VMware HCX-Bereitstellung.

Der HCX WAN Optimization Service wird in Verbindung mit der HCX WAN Interconnect Service Appliance (HCX-IX) bereitgestellt. HCX-IX ist für die Datenreplikation zwischen der Unternehmensumgebung und der Amazon EVS-Umgebung verantwortlich.

Um den HCX WAN Optimization Service mit Amazon EVS zu verwenden, müssen Sie eine verteilte Portgruppe im HCX-VLAN-Subnetz verwenden. Verwenden Sie die verteilte Portgruppe, die im vorherigen Schritt erstellt wurde.

(Optional) Aktivieren Sie HCX Mobility Optimized Networking

HCX Mobility Optimized Networking (MON) ist eine Funktion des HCX Network Extension Service. MON-fähige Netzwerkerweiterungen verbessern den Datenfluss für migrierte virtuelle Maschinen, indem sie selektives Routing innerhalb Ihrer Amazon EVS-Umgebung ermöglichen. MON ermöglicht es Ihnen, den optimalen Pfad für die Migration von Workload-Verkehr zu Amazon EVS zu konfigurieren, wenn Layer-2-Netzwerke gestreckt werden, wodurch ein langer Round-und-Netzwerkpfad durch das Quell-Gateway vermieden wird. Diese Funktion ist für alle Amazon EVS-Bereitstellungen verfügbar. Weitere Informationen finden Sie unter Configuring Mobility Optimized Networking im VMware HCX-Benutzerhandbuch.

> **Important**
>
> Bevor Sie HCX MON aktivieren, lesen Sie die folgenden Einschränkungen und nicht unterstützten Konfigurationen für HCX Network Extension.
> Einschränkungen und Beschränkungen für die Netzwerkerweiterung
> Einschränkungen und Einschränkungen für mobilitätsoptimierte Netzwerktopologien

> **Important**
>
> Bevor Sie HCX MON aktivieren, stellen Sie sicher, dass Sie in der NSX-Schnittstelle die Routenumverteilung für das Zielnetzwerk CIDR konfiguriert haben. Weitere Informationen finden Sie unter Konfigurieren von BGP und Route Redistribution in der NSX-Dokumentation. VMware

Überprüfen Sie die HCX-Konnektivität

VMware HCX enthält integrierte Diagnosetools, mit denen die Konnektivität getestet werden kann. Weitere Informationen finden Sie unter VMware HCX-Fehlerbehebung im VMware HCX-Benutzerhandbuch.

Öffentliche HCX-Internetkonnektivität konfigurieren

Sie können den öffentlichen Internetzugang für Ihr öffentliches HCX-VLAN konfigurieren, indem Sie Elastic IP-Adressen mit Ihrem VLAN verknüpfen. Dies ermöglicht eine direkte Internetverbindung für VMware HCX-Appliances und Workloads, die für Migrationsvorgänge einen Internetzugang benötigen.

Verwandte Themen

Dieses Thema behandelt die Verwaltung des Internetzugangs für das öffentliche HCX-VLAN. Für eine vollständige Implementierung:

1. Vollständige Voraussetzungen inAmazon Elastic VMware Service einrichten.
2. Konfigurieren Sie die Ersteinrichtung inErste Schritte.
3. Internetzugang konfigurieren (dieses Thema).

Über den HCX VLAN-Internetzugang

Sie können den Internetzugang für VMware HCX-Appliances konfigurieren, sodass Sie die HCX-Migration Ihrer Workloads zu Amazon EVS über das Internet durchführen können.

Dieser Ansatz:

- Ermöglicht Migrationen virtueller Maschinen, ohne dass eine spezielle private Konnektivität erforderlich ist.
- Bietet eine flexible, kostengünstige Lösung für die Migration.

> **Important**
>
> Die internetbasierte HCX-Migration wird im Allgemeinen nicht empfohlen für:
>
> - Anwendungen, die empfindlich auf Netzwerkjitter oder Latenz reagieren.
> - Zeitkritische vMotion-Operationen.
> - Umfangreiche Migrationen mit strengen Leistungsanforderungen.
>
> Für diese Szenarien empfehlen wir die Verwendung von HCX Private Connectivity. Eine private, dedizierte Verbindung bietet im Vergleich zu internetbasierten Verbindungen eine zuverlässigere Leistung.

Überblick über die Internetkonnektivität

Sehen Sie sich die folgenden Überlegungen an.

HCX-Netzwerkanforderungen und DNAT

HCX hat spezifische Netzwerkeinschränkungen, die sich darauf auswirken, wie Sie den öffentlichen Internetzugang einrichten.

HCX unterstützt keine Destination Network Address Translation (DNAT). Stattdessen erfordert HCX, dass das Uplink-Netzwerk mit einer Standard-Gateway-IP-Adresse routbar ist.

Amazon EVS VLAN-Subnetze enthalten wie andere VPC-Subnetze eine Standard-Gateway-IP-Adresse. Diese Subnetze sind jedoch immer private Subnetze, auch wenn Sie CIDR-Blöcke außerhalb des Adressbereichs verwenden. RFC1918

HCX-Internetkonnektivität aktivieren

Um Internetkonnektivität ohne DNAT zu ermöglichen, verwendet Amazon EVS einen speziellen CIDR-Konfigurationsansatz:

- Anforderung für routingfähiges Internet: Amazon EVS benötigt ein über das Internet routbares CIDR, das Ihrem HCX-VLAN-Subnetz-CIDR entspricht.
- IPAM-Zuweisung: Amazon EVS verwendet ein öffentliches IPAM-zugewiesenes CIDR mit einer Mindestnetzmaskenlänge von /28 als internetroutbares CIDR.
- VPC-Konfiguration: Sie müssen das öffentliche IPAM-zugewiesene CIDR Ihrer VPC manuell als sekundäres VPC-CIDR hinzufügen.
- VLAN-Subnetz-Bereitstellung: Nachdem IPAM und VPC konfiguriert wurden, können Sie das öffentliche IPAM-zugewiesene CIDR im HCX-VLAN-Subnetz während der Amazon EVS-Bereitstellung verwenden.
- Elastische IP-Konfiguration: Amazon EVS erfordert die folgende Konfiguration:
  - Elastic zuweisen IPs: Sie weisen Elastic IPs aus dem IPAM-zugewiesenen CIDR zu. Sie müssen den HCX Manager- und HCX Interconnect (HCX-IXEIPs) -Appliances mindestens zwei Elastic IP-Adressen () aus dem IPAM-Pool zuweisen. Weisen Sie jeder HCX-Netzwerk-Appliance, die Sie bereitstellen müssen, eine zusätzliche Elastic IP-Adresse zu.
  - Mit VLAN verknüpfen: Sie ordnen jede Elastic IP, die Sie mit einer HCX-Appliance verwenden möchten, dem HCX-VLAN-Subnetz zu. Verwenden Sie die Amazon EVS-Konsole oder AWS CLI für diese Zuordnung.
  - Gateway-Adresse konfigurieren: Die erste verwendbare Adresse aus dem CIDR wird zur Gateway-Adresse, die Sie in Ihrer HCX-Appliance konfigurieren.
  - Traffic-Routing: Der Datenverkehr für jede zugeordnete Elastic IP leitet direkt zur HCX-Ziel-Appliance mit derselben IP-Adresse, ohne DNAT.

Schritte zur Konfiguration von HCX mit Internetkonnektivität für die Bereitstellung einer Amazon EVS-Umgebung finden Sie unter Amazon Elastic VMware Service einrichten und. Erste Schritte

Überlegungen zum Betrieb

- Der öffentliche HCX-VLAN-CIDR-Block muss eine Netzmaskenlänge von /28 haben.
- EIPs können nach der Bereitstellung über die Amazon EVS-Konsole oder dem öffentlichen HCX-VLAN zugeordnet oder von diesem getrennt werden AWS CLI, müssen jedoch aus demselben IPAM-Pool stammen.
- Jede EIP-Zuordnung hat ihre eigene eindeutige Zuordnungs-ID.
- Sie können bis zu 13 EIPs aus einem öffentlichen IPAM-Pool haben, der mit dem öffentlichen HCX-VLAN /28 verknüpft ist. Sie können die ersten beiden EIPs oder die letzten EIP aus dem öffentlichen IPAM-zugewiesenen CIDR-Block nicht dem öffentlichen HCX-VLAN-Subnetz zuordnen. Diese EIPs sind als Netzwerk-, Standard-Gateway- und Broadcast-Adressen reserviert. Amazon EVS gibt einen Validierungsfehler aus, wenn Sie versuchen, diese EIPs mit dem VLAN zu verknüpfen.

Sicherheitsüberlegungen

- Netzwerkzugriffskontrolllisten (ACLs) gelten weiterhin für den Datenverkehr, der durch das öffentliche HCX-VLAN-Subnetz fließt.
- Sicherheitsgruppenregeln gelten nicht für den Verkehr in öffentlichen HCX-VLAN-Subnetzen. Verwenden Sie das Netzwerk ACLs für die Datenverkehrskontrolle.

> **Important**
>
> Wenn Sie eine Verbindung über das Internet herstellen, ermöglicht die Verknüpfung einer Elastic IP-Adresse mit einem VLAN direkten Internetzugriff auf alle Ressourcen in diesem VLAN. Stellen Sie sicher, dass Sie die entsprechenden Listen zur Netzwerkzugriffskontrolle so konfiguriert haben, dass der Zugriff entsprechend Ihren Sicherheitsanforderungen eingeschränkt wird.

Verwaltung von Elastic IP-Adressen für VLANs

Sie können Elastic IP-Adressen mit einem öffentlichen HCX-VLAN über die Amazon EVS-Konsole oder trennen. AWS CLI

> **Note**
>
> Amazon EVS unterstützt derzeit nur das Zuordnen und Trennen von Elastic IP-Adressen zu einem öffentlichen HCX-VLAN.

Ordnen Sie eine Elastic IP-Adresse einem VLAN zu

Voraussetzungen

Stellen Sie sicher, dass Sie über Folgendes verfügen:

- Die elastische IP-Adresse wird aus dem öffentlichen IPAM-Pool von Amazon zugewiesen.
- Die Amazon EVS-Umgebung wurde bereits erstellt.

Example

Amazon EVS console

1. Gehen Sie zur Amazon EVS-Konsole.
2. Wählen Sie im Navigationsmenü Umgebungen aus.
3. Wählen Sie die Umgebung aus.
4. Wählen Sie auf der Registerkarte Netzwerke und Konnektivität das öffentliche HCX-VLAN aus.

   > **Note**
   >
   > Amazon EVS unterstützt derzeit nur die Verbindung EIPs mit dem HCX-VLAN.

5. Wählen Sie EIP mit VLAN verknüpfen aus.
6. Wählen Sie die Elastic IP-Adresse (n) aus, die dem öffentlichen HCX-VLAN zugeordnet werden sollen.
7. Wählen Sie Associate EIPs aus. Sie können bis zu 13 mit EIPs dem öffentlichen HCX-VLAN verknüpfen.

> **Note**
>
> Sie können die ersten beiden EIPs aus dem öffentlichen IPAM-CIDR-Block nicht dem VLAN-Subnetz zuordnen. Diese EIPs sind als Netzwerk- und Standard-Gateway-Adressen reserviert.

8. Überprüfen Sie die EIP-Verknüpfungen, um sicherzustellen, dass sie mit dem öffentlichen HCX-VLAN verknüpft EIPs wurden.

AWS CLI

1. Verwenden Sie den Beispielbefehl, um eine Elastic IP-Adresse einem VLAN zuzuordnen. `associate-eip-to-vlan`
   - `environment-id`- Die ID Ihrer Amazon EVS-Umgebung.
   - `vlan-name`- Muss sein. `hcx` Amazon EVS unterstützt derzeit nur die EIP-Verbindung mit dem HCX-VLAN.
   - `allocation-id`— Die Zuweisungs-ID der Elastic IP-Adresse.

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

   Der Befehl gibt Details zum VLAN zurück, einschließlich der neuen EIP-Zuordnung:

   ```
   {
       "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"
    }
}
```

Das `eipAssociations` Array zeigt die neue Assoziation, einschließlich:

- `associationId`- Die eindeutige ID für diese EIP-Assoziation, die für die Trennung der Verbindung verwendet wird.
- `allocationId`— Die Zuweisungs-ID der zugehörigen Elastic IP-Adresse.
- `ipAddress`- Die dem VLAN zugewiesene IP-Adresse.

2. Wiederholen Sie den Schritt, um weitere EIPs Verbindungen herzustellen. Sie können bis zu 13 mit EIPs dem öffentlichen HCX-VLAN verknüpfen.

Trennen Sie eine Elastic IP-Adresse von einem VLAN

Voraussetzungen

Stellen Sie sicher, dass Sie über Folgendes verfügen:

- Die Amazon EVS-Umgebung wurde bereits erstellt.
- EIP ist mit der Amazon EVS-Umgebung verknüpft.

Example

Amazon EVS console

1. Gehen Sie zur Amazon EVS-Konsole.
2. Wählen Sie im Navigationsmenü Umgebungen aus.
3. Wählen Sie die Umgebung aus.
4. Wählen Sie auf der Registerkarte Netzwerke und Konnektivität das öffentliche HCX-VLAN aus.
5. Wählen Sie EIP vom VLAN trennen.

6. Wählen Sie die Elastic IP-Adresse (n) aus, die Sie vom öffentlichen HCX-VLAN trennen möchten.

> **Important**
>
> Die Trennung EIPs kann zu einem Verlust der Internetverbindung für Appliances führen, die öffentliche VLAN-Subnetze verwenden.

7. Wählen Sie Disassociate (Zuordnung aufheben) EIPs aus.
8. Überprüfen Sie die EIP-Zuordnungen, um sicherzustellen, dass sie vom öffentlichen EIPs HCX-VLAN getrennt wurden.

AWS CLI

Verwenden Sie den Beispielbefehl, um die Zuordnung einer Elastic IP-Adresse zu einem VLAN zu trennen. `disassociate-eip-from-vlan`

- `environment-id`- Die ID Ihrer Amazon EVS-Umgebung.
- `vlan-name`- Muss sein. `hcx` Amazon EVS unterstützt derzeit nur die EIP-Verbindung mit dem HCX-VLAN.
- `association-id`— Die Zuordnungs-ID der EIP-Zuordnung, die entfernt werden soll.

> **Important**
>
> Das Trennen der Zuordnung EIPs kann zu einem Verlust der Internetverbindung für Appliances führen, die öffentliche VLAN-Subnetze verwenden.

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

Der Befehl gibt Details über das VLAN zurück, bei dem die EIP-Zuordnung entfernt wurde:

```
{
    "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"
    }
}
```


Das leere `eipAssociations` Array bestätigt, dass die Elastic IP-Adresse erfolgreich vom VLAN getrennt wurde.

Über HCX WAN-Optimierung für internetbasierte Migrationen

> **Note**
>
> Die WAN-Optimierungsfunktion ist in HCX 4.11.3 nicht mehr verfügbar. Weitere Informationen finden Sie in den Versionshinweisen zu HCX 4.11.3.

Bei Migrationen über das Internet kann HCX WAN Optimization (HCX-WO) die Migrationsleistung verbessern. Der Dienst funktioniert in Verbindung mit der HCX Interconnect-Appliance (HCX-IX), um:

- Wenden Sie Techniken zur Datenreduzierung an, um die Bandbreitennutzung zu minimieren.
- Implementieren Sie die WAN-Pfadkonditionierung, um die Netzwerkleistung zu optimieren.
- Verbessern Sie die Migrationsgeschwindigkeit bei Internetverbindungen mit hoher Latenz.
- Verbessern Sie die Zuverlässigkeit internetbasierter Migrationen.

Die HCX-WAN-Optimierung ist besonders nützlich für internetbasierte Migrationen, bei denen:

- Die Netzwerklatenz kann höher sein als bei privaten Verbindungsoptionen.
- Die verfügbare Bandbreite kann begrenzt oder variabel sein.
- Die Netzwerkbedingungen können aufgrund der Muster des Internetverkehrs schwanken.

Ausführliche Anweisungen zur Einrichtung der HCX-WAN-Optimierung nach der Konfiguration der Internetverbindung finden Sie unter. the section called “(Optional) Richten Sie die HCX-WAN-Optimierung ein”

> **Note**
>
> Die WAN-Optimierung kann zwar die Leistung der internetbasierten Migration erheblich verbessern, bietet jedoch in Umgebungen mit dedizierten 10-Gbit-Verbindungen mit niedriger Latenz möglicherweise keine zusätzlichen Vorteile. Berücksichtigen Sie Ihre Netzwerkeigenschaften, wenn Sie entscheiden, ob Sie diese Funktion aktivieren möchten.

Verwaltung von Amazon EVS-Umgebungen

Dieses Kapitel enthält die folgenden Themen, die Ihnen bei der Verwaltung Ihrer Umgebung helfen sollen.

- the section called “VCF-Abonnements”- Beschreibt, wie VCF-Abonnements mit Amazon EVS funktionieren, und beschreibt die Verantwortung des Kunden für die VCF-Abonnementverwaltung.
- the section called “VCF-Versionen und EC2-Instances”— Beschreibt die unterstützten VCF- und ESX-Versionen und wie Sie die Versionsverfügbarkeit in Amazon EVS überprüfen können.
- the section called “Lebenszyklusmanagement”- Beschreibt die Verantwortlichkeiten für das Lebenszyklusmanagement innerhalb einer Amazon EVS-Umgebung, einschließlich des zugrunde liegenden Infrastrukturmanagements, des VCF-Upgrade-Managements und des ESX-Host-Lebenszyklusmanagements.
- the section called “Wartung der Umgebung”- Beschreibt, wie Sie allgemeine Wartungsaufgaben für Ihre Amazon EVS-Umgebung durchführen, einschließlich Netzwerkkonfiguration, ESX-Host-Wartung, Überprüfung des Umgebungsstatus und Verwaltung geheimer Rotationspläne für Ihre VCF-Anmeldeinformationen.
- the section called “Host erstellen”— Beschreibt, wie Sie nach der Bereitstellung der Umgebung einen Amazon EVS-Host erstellen und den Host dem Cluster hinzufügen.
- the section called “Host löschen”— Beschreibt, wie ein Amazon EVS-Host gelöscht und aus dem Cluster entfernt wird.
- the section called “Konnektor erstellen”— Beschreibt, wie ein Amazon EVS-Umgebungsconnector erstellt wird, um eine dauerhafte Verbindung zwischen Amazon EVS und einer VCF-Appliance herzustellen.
- the section called “Konnektor aktualisieren”— Beschreibt, wie ein Amazon EVS-Umgebungsconnector aktualisiert wird, um den FQDN oder Secrets Manager Manager-Schlüssel der Appliance zu ändern.
- the section called “Konnektor löschen”— Beschreibt, wie ein Amazon EVS-Umgebungsconnector gelöscht wird.
- the section called “Anspruch erstellen”— Beschreibt, wie Sie eine Amazon EVS-Berechtigung einrichten, um die AWS angebotene Windows-Lizenzierung für zu aktivieren. VMs
- the section called “Anspruch löschen”— Beschreibt, wie eine Amazon EVS-Berechtigung gelöscht wird, um den AWS angebotenen Windows-Lizenzierungsschutz zu entfernen. VMs

- the section called “Konfigurieren Sie die Windows Server-Aktivierung”— Beschreibt, wie die Windows Server-Aktivierung auf Geräten konfiguriert wird VMs , die über Windows Server-Berechtigungen verfügen.

VCF-Abonnements

> **Note**
>
> Amazon EVS unterstützt keine unbefristeten vSphere-Lizenzen. Sie benötigen ein gültiges und aktives VMware Cloud Foundation-Abonnement, um Amazon EVS nutzen zu können.

Amazon EVS verwendet VMware Cloud Foundation (VCF) -Abonnements mit Lizenzportabilitätsberechtigungen, die Sie mitbringen AWS (BYOS). Um eine Amazon EVS-Umgebung erfolgreich bereitzustellen, müssen Sie in der Anfrage zur Umgebungserstellung einen gültigen VCF-Lösungsschlüssel und einen vSAN-Lizenzschlüssel angeben. Der vSphere-Lizenzschlüssel dient als Lösungsschlüssel für VCF. Jeder VCF-Lizenzschlüssel kann nur für eine Amazon EVS-Umgebung verwendet werden. Die Erstellung einer Umgebung schlägt fehl, wenn Sie versuchen, einen VCF-Lizenzschlüssel zu verwenden, der bereits in einer anderen Umgebung verwendet wird.

Ihr VCF-Lösungsschlüssel muss über genügend Kerne verfügen, um eine angemessene Kernkapazität für die vier ersten EC2-Hosts bereitzustellen, die Amazon EVS bei der Erstellung der Umgebung bereitstellt. Die erforderliche Anzahl an Kernen hängt vom ausgewählten Instance-Typ ab, da jeder Instance-Typ eine unterschiedliche Anzahl von Kernen hat.

Instance-Typ	Kerne pro Host	Mindestanzahl Kerne für 4 Hosts (VCF-Lizenz)
i4i.metal	64	256
i7i.metal-24xl	48	192

Der vSAN-Lizenzschlüssel muss die instance-type-specific Kapazitätsanforderungen erfüllen. Die erforderliche Kapazität hängt vom ausgewählten Instanztyp ab:

Instance-Typ	Minimale vSAN-Kapazität für 4 Hosts (vSAN-Lizenz)
i4i.metal	110 TiB
i7i.metal-24xl	82 TiB

Die Erstellung der Umgebung schlägt fehl, wenn Sie versuchen, unterdimensionierte Lizenzschlüssel zu verwenden.

> **Note**
>
> Ihr VCF-Abonnement steht Amazon EVS in allen AWS Regionen zur Verfügung, um die Einhaltung der Lizenzbestimmungen zu gewährleisten. Amazon EVS validiert keine Lizenzschlüssel. Besuchen Sie den Broadcom-Support, um Lizenzschlüssel zu validieren.

> **Note**
>
> Informationen über Ihre VCF-Software in Amazon EVS werden an Broadcom weitergegeben, um die Einhaltung der Lizenzbestimmungen zu überprüfen.

Abonnementverwaltung

Sie sind für die Verwaltung Ihrer VCF-Abonnements verantwortlich. Ihre VCF-Abonnements müssen im SDDC Manager verwaltet werden. Wenn Sie Ihre Lizenzschlüssel aus dem SDDC Manager entfernen oder sie durch einen verwendeten Lizenzschlüssel ersetzen, führt dies zu einer fehlgeschlagenen Überprüfung des Umgebungsstatus, sodass Sie Ihrer Amazon EVS-Umgebung keine Hosts hinzufügen können. Weitere Informationen zu Prüfungen des Umgebungsstatus und. the section called “Überwachen Sie den Status der Umgebung” the section called “Beheben Sie fehlgeschlagene Umgebungsstatusprüfungen” Weitere Informationen zu VCF-Lizenzschlüsseln finden Sie unter Verwaltung von Lizenzschlüsseln in VMware Cloud Foundation in der VMware Cloud Foundation-Dokumentation.

> **Important**
>
> Verwenden Sie die SDDC Manager-Benutzeroberfläche, um die VCF-Lösung und die vSAN-Lizenzschlüssel zu verwalten. Amazon EVS erfordert, dass Sie gültige VCF-Lösungs- und vSAN-Lizenzschlüssel im SDDC Manager verwalten, damit der Service ordnungsgemäß funktioniert. Schlüssel müssen Ihren Hosts und dem vSAN-Cluster zwar mithilfe des vSphere Client zugewiesen werden, Sie müssen jedoch sicherstellen, dass diese Schlüssel auch auf dem Lizenzierungsbildschirm der SDDC Manager-Benutzeroberfläche angezeigt werden.

Hinzufügen von VCF-Lizenzschlüsseln

Im Broadcom-Supportportal können Sie zusätzliche VCF-Lizenzschlüssel erwerben, Lizenzschlüssel aufteilen, falls Sie bereits über große Schlüssel verfügen, oder mehrere Lizenzschlüssel zusammenführen. Auf diese Weise können Sie Hosts lizenzieren, die Sie nach der ersten Bereitstellung zu Ihrer Umgebung hinzugefügt haben, oder zusätzliche Umgebungen lizenzieren. Stellen Sie sicher, dass die gekauften Lizenzschlüssel dem vCenter Server- und SDDC Manager-Inventar hinzugefügt wurden. Wenn Sie Hosts hinzufügen, stellen Sie sicher, dass Ihre Lizenzen den richtigen Hosts in vSphere zugewiesen sind und über ausreichende Kerne und vSAN-Speicherkapazität verfügen. Amazon EVS unterstützt keine Hosts ohne Lizenz. Weitere Informationen finden Sie in der VMware Dokumentation unter Konfiguration von Lizenzeinstellungen für Assets im vSphere Client.

Neue, noch nicht abgelaufene Lizenzschlüssel müssen vCenter Server zugewiesen werden, bevor der Testzeitraum des Lizenzschlüssels abläuft, um aktiv zu bleiben. Aktive Lizenzschlüssel sind erforderlich, um eine Amazon EVS-Umgebung erfolgreich einzurichten. Ihre Umgebung kann nicht bereitgestellt werden, wenn ein abgelaufener Lizenzschlüssel bereitgestellt wird. Weitere Informationen zur Erstellung eines VCF-Lizenzschlüssels finden Sie in der VMware Dokumentation unter Neue Lizenz erstellen. Wenn Sie Probleme mit Ihren hinzugefügten Lizenzschlüsseln haben, finden Sie weitere Informationen unterthe section called “Die Überprüfung der Schlüsselabdeckung ist fehlgeschlagen”.

VCF-Lizenzschlüssel entfernen

Sie können VCF-Lizenzschlüssel aus dem SDDC Manager-Inventar entfernen, um Ihre Kern- und vSAN-Kapazität nach dem Löschen von Hosts in Ihrer Umgebung zu reduzieren. Um die Lizenzmodelle der Produkte, die Sie mit vSphere verwenden, einzuhalten, müssen Sie alle nicht

zugewiesenen Lizenzschlüssel aus der Bestandsliste entfernen. Wenn Sie Lizenzschlüssel im Broadcom Support Portal aufgeteilt, zusammengeführt oder aktualisiert haben, müssen Sie die alten Lizenzschlüssel entfernen. Weitere Informationen finden Sie in der VMware Dokumentation unter Eine Lizenz entfernen.

Von Amazon EVS bereitgestellte VCF-Versionen und EC2-Instance-Typen

Amazon EVS bietet mehrere Versionen der Instanztypen VMware Cloud Foundation (VCF), ESX und EC2, die Sie beim Erstellen einer Umgebung und beim Erstellen eines Hosts auswählen können.

Überprüfung der bereitgestellten VCF-Versionen, ESX-Versionen und EC2-Instance-Typen

Die AWS Konsole zeigt die Liste der VCF-Versionen, die von Amazon EVS im Assistenten zum Erstellen einer Umgebung bereitgestellt werden. Die verfügbaren ESX-Versionen sind sichtbar, wenn Sie beim Hinzufügen eines Hosts zu einer vorhandenen Umgebung einen Instance-Typ auswählen. Sie können auch VCF-Versionen, ESX-Versionen und EC2-Instance-Typen mithilfe der CLI anzeigen.

Example

Amazon EVS console

1. Gehen Sie zur Amazon EVS-Konsole.
2. Wählen Sie im Navigationsmenü Umgebungen aus.
3. Führen Sie eine der folgenden Aktionen aus:

   Um VCF-Versionen zu überprüfen:

   a. Wählen Sie Umgebung erstellen aus.
   b. Wählen Sie unter den Anforderungen zur Validierung von Amazon EVS Ihre VCF-Version aus, um zu sehen, ob der Status für Sie verfügbar oder eingeschränkt ist.

   So überprüfen Sie die ESX-Versionen:

   a. Wählen Sie eine bestehende Umgebung aus.
   b. Wählen Sie Create hoste (Host erstellen) aus.
   c. Wählen Sie einen Instanztyp aus, um die verfügbaren ESX-Versionen zu sehen.

AWS CLI

Führen Sie den folgenden Befehl aus, um Informationen zu VCF- und ESX-Versionen abzurufen:

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

Beispielantwort:

```
{
    "vcfVersions": [
        {
            "vcfVersion": "VCF-5.2.1",
            "status": "RESTRICTED",
            "defaultEsxVersion": "ESXi-8.0U3b-24280767",
            "instanceTypes": [
                "i4i.metal",
                "i7i.metal-24xl"
            ]
        },
        {
            "vcfVersion": "VCF-5.2.2",
            "status": "AVAILABLE",
            "defaultEsxVersion": "ESXi-8.0U3g-24859861",
            "instanceTypes": [
                "i4i.metal",
                "i7i.metal-24xl"
            ]
        }
    ],
    "instanceTypeEsxVersions": [
        {
            "instanceType": "i4i.metal",
            "esxVersions": [
                "ESXi-8.0U3b-24280767",
                "ESXi-8.0U3g-24859861"
            ]
        },
        {
            "instanceType": "i7i.metal-24xl",
            "esxVersions": [
                "ESXi-8.0U3b-24280767",
                "ESXi-8.0U3g-24859861"
            ]
```

```
        }
    ]
}
```

> **Note**
>
> Wenn die Version, die Sie benötigen`RESTRICTED`, angezeigt wird und Sie einen bestimmten Bedarf haben, finden the section called “Zugriff auf eingeschränkte VCF-Versionen beantragen” Sie weitere Informationen zum Zugriff auf diese Version unter.

Aktuelle VCF-Versionen in Amazon EVS

Amazon EVS bietet derzeit die folgenden VCF-Versionen für die Umgebungserstellung:

VCF-Version	ESX-Standardversion	Status	EC2-Instance-Typen
VCF-5.2.2	ESXi-8,0u3G-24859861	VERFÜGBAR	i4i.metall, i7i.metall-24xl
VCF-5.2.1	ESXi-8,0U3B-24280767	BESCHRÄNKT	i4i.metal, i7i.metal-24xl

> **Note**
>
> Wenn Sie eine neue Amazon EVS-Umgebung erstellen, müssen Sie eine VCF-Version angeben.

Überlegungen zur ESX-Version

Jede VCF-Version hat eine ESX-Standardversion, die auf der Broadcom VCF-Stückliste (BOM) basiert. Beim Erstellen einer neuen Umgebung können Sie keine bestimmte ESX-Version auswählen. Die ESX-Standardversion für die ausgewählte VCF-Version wird automatisch angewendet.

Wenn Sie Ihrer Umgebung jedoch einen Host hinzufügen, können Sie eine verfügbare ESX-Version für den von Ihnen ausgewählten Instance-Typ auswählen. Wenn Sie keine angeben, verwendet Amazon EVS die ESX-Standardversion, die der VCF-Version Ihrer Umgebung zugeordnet ist.

Nachdem ein Host hinzugefügt wurde, kann seine ESX-Version nur mit vCenter Lifecycle Manager aktualisiert werden.

> **Note**
>
> Amazon EVS bietet nicht alle von Broadcom veröffentlichten Versionen von VCF und ESX. Informationen zur Software-Interoperabilität finden Sie in der Broadcom Interoperability Matrix. Informationen zur vollständigen Hardwarekompatibilität mit AWS EC2-Instances finden Sie im Broadcom Compatibility Guide.

Zugriff auf eingeschränkte VCF-Versionen beantragen

Wenn Sie Zugriff auf eine VCF-Version mit einem `RESTRICTED` Status benötigen, wenden Sie sich mit den folgenden Informationen an den AWS Support:

- Ihre AWS Konto-ID
- Die AWS Region
- Die spezifische VCF-Version, die Sie benötigen
- Ihr Anwendungsfall und Ihre geschäftliche Begründung (z. B.security/compliance, compatibility/dependency, und andere)

AWS Der Support wird Ihre Anfrage prüfen und entweder genehmigen oder zusätzliche Informationen anfordern. Nach der Genehmigung ändert sich der Versionsstatus `AVAILABLE` in der AWS Konsolen- oder `get-versions` API-Antwort auf.

Lebenszyklusmanagement der Amazon EVS-Umgebung

Auf dieser Seite werden Ihre Lifecycle-Management-Aufgaben in einer Amazon EVS-Umgebung beschrieben.

Ein wesentlicher Vorteil von Amazon EVS besteht darin, dass Sie die vollständige Kontrolle über Ihre VMware Architektur in der Cloud haben. Sie können den VMware Cloud Foundation (VCF) -Softwarestack optimieren, um den individuellen Anforderungen Ihrer Anwendungen gerecht zu

werden. Da es sich bei Amazon EVS um einen selbstverwalteten Service handelt, sind Sie für das Lebenszyklusmanagement und die Wartung der in der Amazon EVS-Umgebung verwendeten VMware Software wie ESX, vSphere, vSAN, NSX und SDDC Manager verantwortlich. Sie sind auch dafür verantwortlich, Integrationen von Drittanbietern aufrechtzuerhalten, z. B. Datenschutzlösungen, die Sie in Ihre Amazon EVS-Hosts integrieren.

Sie sind verantwortlich für die Konfiguration der zugrunde liegenden AWS Netzwerkkomponenten, die Amazon EVS verwendet, einschließlich VPC-Routentabellen, Sicherheitsgruppen- und ACL-Regeln (Network Access Control List), VPC-Routenserver-Konfiguration, Internet-Gateways, NAT-Gateways und Transit-Gateways (für lokale Konnektivität).

AWS ist verantwortlich für die Bereitstellung der Amazon EVS-Umgebung mit den von Ihnen bereitgestellten Netzwerkkonfigurationen. Die Bereitstellung der Umgebung umfasst Folgendes:

- Bootstrapping der Netzwerkkonfiguration Ihrer Amazon EVS-Umgebung.
- Aktivieren von Nord-Süd-Routing mit der von Ihnen bereitgestellten VPC-Route-Server-Instanz.
- Bereitstellung der erforderlichen EVS-VLAN-Subnetze, elastischen Netzwerkschnittstellen und vier anfänglichen ESX-Hosts.
- Konfiguration eines NSX-Overlay-Netzwerks mit einem Tier-0-Gateway und einem Tier-1-Gateway.
- Bereitstellung eines NSX Edge-Clusters mit zwei NSX Edge-Knoten im Modus. Active/Standby
- Erstellen und Konfigurieren des ersten vSAN-Clusters und Mounten des Datenspeichers.

Sie sind verantwortlich für die VMware NSX-Konfiguration, einschließlich Netzwerksegmente, verteilter Firewallregeln und Load Balancer. Sie sind auch für die Konfiguration aller integrierten Lösungen verantwortlich, die Sie nach der Bereitstellung der EVS-Umgebung mit Amazon EVS implementieren, einschließlich der VMware HCX-Konfiguration und zusätzlicher NSX Tier-1-Gateways.

Weitere Informationen zu AWS und zu den Verantwortlichkeiten der Kunden finden Sie im Modell der gemeinsamen Verantwortung.AWS

> **Note**
>
> Ein Tier-0-Gateway und ein Tier-1-Gateway werden im Rahmen der Bereitstellung der Amazon EVS-Umgebung erstellt und konfiguriert. Amazon EVS unterstützt derzeit nur ein einziges Tier-0-Gateway. Jede Änderung an diesen logischen Routern oder dem NSX Edge-Knoten VMs könnte die Konnektivität beeinträchtigen und sollte vermieden werden.

VMware Softwareupdates

> **Warning**
>
> Wenn Sie Ihre ESX-Version nach der Bereitstellung der Amazon EVS-Umgebung aktualisiert haben, schlägt der SDDC-Manager möglicherweise bei der VCF-Host-Validierung im Schritt Provision-Hosts fehl. Schritte zur Behebung dieses Problems finden Sie unter. the section called “SDDC Manager schlägt die VCF-Hostvalidierung bei der Host-Inbetriebnahme fehl”

Informationen zu den von Amazon EVS bereitgestellten VCF-Versionen finden Sie unter. the section called “VCF-Versionen und EC2-Instances” Gemäß dem Modell der AWS gemeinsamen Verantwortung sind Sie dafür verantwortlich, alle Patches, Updates oder Upgrades für VCF-Software, einschließlich ESX, vCenter Server, vSAN, NSX, SDDC Manager und andere integrierte Lösungen, in Ihrer EVS-Umgebung anzuwenden. Nach der Bereitstellung empfehlen wir Ihnen, die von Amazon EVS bereitgestellte VCF-Softwareversion zu überprüfen und bei Bedarf zu aktualisieren. Sie können VCF-Updates über das Broadcom-Supportportal erhalten. Wir empfehlen Ihnen außerdem, einen regelmäßigen Wartungsplan für Updates und Patches festzulegen und einzuhalten.

> **Note**
>
> Amazon EVS unterstützt VMware Cloud Foundation 9 derzeit nicht.

> **Note**
>
> Amazon EVS stellt nicht alle von Broadcom veröffentlichten Versionen von VCF und ESX zur Verfügung. Informationen zur Software-Interoperabilität finden Sie in der Broadcom Interoperability Matrix. Informationen zur vollständigen Hardwarekompatibilität mit AWS EC2-Instances finden Sie im Broadcom Compatibility Guide.

Bestimmte Patches, Updates oder Upgrades können sich auf Workloads auswirken, die in Ihrer Umgebung ausgeführt werden. Bevor Sie Ihre VCF-Software patchen, aktualisieren oder aktualisieren, empfehlen wir Ihnen, den VCF Lifecycle Management Guide zu lesen, um zu erfahren, wie sich diese Änderungen auf Ihre Umgebung auswirken werden. Wir empfehlen außerdem, Änderungen in einer Staging-Umgebung zu testen, bevor Sie sie in der Produktionsumgebung

einsetzen. Sie können die Versionshinweise zu VCF 5.2.x lesen, um mehr über die neuesten VCF 5.2.x-Updates zu erfahren.

Lebenszyklus und Wartung des ESX-Hosts

Sie sind verantwortlich für die Verwaltung und Wartung des ESX-Host-Lebenszyklus innerhalb der Amazon EVS-Umgebung, einschließlich der Überwachung des Hostzustands und der Behebung von Hostproblemen. Weitere Informationen finden Sie unter the section called “Wartung der Umgebung”.

AWS führt geplante Wartungsarbeiten an den zugrunde liegenden EC2-Metal-Instances durch, um die Zuverlässigkeit, Verfügbarkeit und Leistung der Infrastruktur sicherzustellen. Weitere Informationen finden Sie unter the section called “Informationen zu AWS geplanten Wartungsarbeiten für EC2-Instances”.

Durchführung von Wartungsarbeiten an Ihrer Umgebung

In diesem Abschnitt wird beschrieben, wie Sie allgemeine Wartungsaufgaben für Ihre Amazon EVS-Umgebung durchführen.

Themen

- Überwachen Sie den Status und die Ressourcen Ihrer Umgebung
- AMI-Wartung
- Wartung des Amazon EVS-Hosts
- Konfigurieren Sie eine benutzerdefinierte Routing-Tabelle für Amazon EVS-Subnetze
- Konfiguration einer Netzwerkzugriffskontrollliste zur Steuerung des Amazon EVS-VLAN-Subnetzverkehrs
- Geheimer Verwaltungslebenszyklus

Überwachen Sie den Status und die Ressourcen Ihrer Umgebung

Sie können verschiedene Aspekte Ihrer Amazon EVS-Umgebung und der zugrunde liegenden AWS Ressourcen mithilfe der Amazon EVS-Konsole oder überwachen. AWS CLI

> **Note**
>
> VMware Cloud Foundation (VCF) -Komponenten werden im SDDC Manager überwacht. Sie können VCF-Komponenten nicht mit der Amazon EVS-Konsole oder überwachen. AWS CLI

Informationen zur Verwendung von SDDC Manager zur Überwachung von VMware Cloud Foundation (VCF) -Komponenten finden Sie unter Erste Schritte mit SDDC Manager.

Umgebungsstatus und Ressourcen anzeigen

Anhand des Umgebungsstatus können Sie feststellen, ob in Ihrer Umgebung Probleme auftreten, die behoben werden müssen. Gehen Sie wie folgt vor, um den Status Ihrer Umgebung zu überprüfen und die zugrunde liegenden Ressourcen einzusehen.

Example

Amazon EVS console

1. Öffnen Sie die Amazon EVS-Konsole.
2. Wählen Sie im Navigationsbereich Environments (Umgebungen) aus.
3. Wählen Sie Ihre Umgebungs-ID, um die Seite mit den Umgebungsdetails zu öffnen.
4. Sehen Sie sich unter Details den Status der Umgebung an.

   Wenn Ihre Umgebung fehlerfrei ist, wird der Status als Bestanden angezeigt. Wenn es Probleme gibt, wird der Status als Fehlgeschlagen angezeigt. Wenn der Status Fehlgeschlagen lautet, können Sie sich ein Popover ansehen, in dem die Ergebnisse von vier Umgebungsstatusprüfungen angezeigt werden:

   - Wiederverwendung von Schlüsseln — Zeigt „Bestanden“ oder „Fehlgeschlagen“ an, um anzuzeigen, ob der VCF-Lizenzschlüssel gültig ist.
   - Hostanzahl — Zeigt „Unbekannt“, „Bestanden“ oder „Fehlgeschlagen“ an, um den Status der Host-Konnektivität anzuzeigen.
   - Schlüsselabdeckung — Zeigt „Bestanden“ oder „Fehlgeschlagen“ an, um anzuzeigen, ob der VCF-Lizenzschlüssel für alle Hosts gilt.
   - Erreichbarkeit — Zeigt „Bestanden“ oder „Fehlgeschlagen“ an, um die Erreichbarkeit für SDDC Manager anzuzeigen.

     Informationen zur Behebung von Fehlern bei der Überprüfung des Umgebungsstatus finden Sie unter. Fehlerbehebung

     So zeigen Sie die Ressourcen in Ihrer Umgebung an

     Wählen Sie eine der folgenden Registerkarten:

- Hosts — Zeigt die Hosts in Ihrer Umgebung an.
- Netzwerke und Konnektivität — Zeigt die VPC-, EVS-Subnetze und VPC-Routenserver-Ressourcen an, die mit Ihrer Umgebung verknüpft sind.
- Verwaltungs-Appliances — Zeigt die VCF-Verwaltungs-Appliances in Ihrer Umgebung mit ihren DNS-Hostnamen und den zugehörigen Anmeldeinformationen an.
- Tags — Zeigt die mit Ihrer Umgebung verknüpften Tags an.

AWS CLI

Sie können den verwenden AWS CLI , um den Status und die Ressourcen Ihrer Umgebung zu überprüfen.

Um alle Umgebungen und ihren Status aufzulisten

```
aws evs list-environments
```

> **Tip**
>
> Verwenden Sie den `--query` Parameter, um die Ausgabe zu filtern. Beispiel:

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

Um Umgebungshosts aufzulisten

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

Um die Umgebung aufzulisten VLANs

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

Weitere Informationen zu den API-Vorgängen finden Sie im Amazon EVS API-Referenzhandbuch im Folgenden:

- ListEnvironments

- ListEnvironmentHosts
- ListEnvironmentVlans

AMI-Wartung

Amazon EVS stellt ESX-Hosts mit einem benutzerdefinierten EVS Amazon Machine Image (AMI) bereit. Das AMI enthält ein benutzerdefiniertes Hersteller-Add-on, das die erforderlichen Pakete für die Ausführung von ESX auf Amazon EC2 enthält.

Beheben Sie den Fehler beim Hinzufügen eines Hosts aufgrund eines inkompatiblen Cluster-Images

Wenn Sie Ihrer Umgebung einen Host hinzufügen, verfügt der Host über die neueste verfügbare Version des benutzerdefinierten EVS-Add-ons. Wenn Ihre Umgebung Hosts mit einer älteren Add-On-Version verwendet, schlägt das Hinzufügen neuer Hosts fehl und es wird die Fehlermeldung angezeigt, dass der neue Host nicht mit Ihrem Cluster-Image kompatibel ist. Ausführliche Schritte zur Behebung dieses Problems finden Sie unterthe section called “Fehler beim Hinzufügen eines Hosts aufgrund eines inkompatiblen Cluster-Images”.

Wartung des Amazon EVS-Hosts

Da es sich bei Amazon EVS um einen selbstverwalteten Service handelt, sind Sie für die Wartung der VMware Cloud Foundation (VCF) -Software verantwortlich, die auf dem Host ausgeführt wird, die Überwachung des Hostzustands und die Behebung von Hostproblemen, einschließlich des Host-Austauschs bei einem Hostausfall. Weitere Informationen zur Verwaltung von ESX-Hosts in VMware Cloud Foundation (VCF) finden Sie in der Cloud Foundation-Dokumentation unter Hostverwaltung. VMware

Überprüfen des Zustands der zugrunde liegenden EC2-Instanz

Amazon EC2 führt automatisierte Prüfungen bei jeder laufenden EC2-Instance durch, um Hardware- und Softwareprobleme zu identifizieren. Sie können die Ergebnisse dieser Statusprüfungen in der EC2-Konsole einsehen oder AWS CLI um spezifische und erkennbare Probleme zu identifizieren. Weitere Informationen finden Sie unter Statusprüfungen für Amazon EC2 EC2-Instances anzeigen im Amazon EC2 EC2-Benutzerhandbuch und describe-instance-statusin der AWS CLI Befehlszeilenreferenz.

Sie können einen CloudWatch Alarm einrichten, der Sie warnt, wenn die Statusprüfungen bei einer bestimmten Instance fehlschlagen. Weitere Informationen finden Sie im Amazon EC2-

Benutzerhandbuch unter CloudWatch Alarme für Amazon EC2 EC2-Instances erstellen, die die Statusprüfungen nicht bestehen.

Informationen zu AWS geplanten Wartungsarbeiten für EC2-Instances

AWS führt geplante Wartungsarbeiten an den zugrunde liegenden EC2-Instances durch, um Zuverlässigkeit, Verfügbarkeit und Leistung sicherzustellen. EC2-Bare-Metal-Instances unterliegen denselben Arten von geplanten Ereignissen wie andere EC2-Instances. AWS kann Ereignisse planen, um Ihre Instances aufgrund von Hardwareproblemen oder geplanten Wartungsarbeiten neu zu starten, zu stoppen und außer Betrieb zu nehmen. Diese Ereignisse treten nicht häufig auf. Weitere Informationen finden Sie unter Arten von geplanten Veranstaltungen im Amazon EC2 EC2-Benutzerhandbuch.

> **Note**
>
> Sie sollten Ihre Hosts vor einem geplanten Neustart im vSphere Client in den Wartungsmodus versetzen.

Wenn eine Ihrer Instanzen von einem geplanten Ereignis betroffen sein wird, werden Sie vorab per E-Mail über die E-Mail-Adresse AWS benachrichtigt, die mit Ihrer verknüpft ist. AWS-Konto AWS sendet auch ein AWS Gesundheitsereignis, das Sie mithilfe von Amazon überwachen und verwalten können EventBridge. Weitere Informationen finden Sie unter Überwachen von Ereignissen in AWS Health with Amazon EventBridge und Geplante Ereignisse für Amazon EC2 EC2-Instances im Amazon EC2 EC2-Benutzerhandbuch.

Sie können die Veranstaltung jederzeit verschieben, sodass sie an einem bestimmten Datum und zu einer für Sie passenden Uhrzeit stattfindet. Der Zeitplan des Ereignisses kann bis hin zum Ablaufdatum der Ereignisfrist geändert werden. Weitere Informationen finden Sie unter Ein geplantes Ereignis für eine EC2-Instance neu planen im Amazon EC2 EC2-Benutzerhandbuch.

Nutzung von EC2-Kapazitätsreservierungen auf Abruf

Sie können EC2 On-Demand-Kapazitätsreservierungen verwenden, um sicherzustellen, dass Ihr Cluster während der Wartungsperioden über ausreichend Kapazität verfügt. Sie können Kapazität in bestimmten Availability Zones für einen beliebigen Zeitraum reservieren. Weitere Informationen finden Sie unter Reservieren von Rechenkapazität mit EC2-On-Demand-Kapazitätsreservierungen im Amazon EC2 EC2-Benutzerhandbuch.

Die Schritte zum Erstellen einer Kapazitätsreservierung finden Sie unter Erstellen einer Kapazitätsreservierung im Amazon EC2 EC2-Benutzerhandbuch.

> **Note**
>
> Wenn Sie EC2 On-Demand-Kapazitätsreservierungen oder EC2 Dedicated Hosts verwenden, empfehlen wir Ihnen, einen Reserve-Host für geschäftskritische Workloads beizubehalten. Kapazitätsreservierungen stellen zwar sicher, dass Sie Zugriff auf eine bestimmte Menge an EC2-Instance-Kapazität in einer bestimmten Availability Zone haben, aber ein Reserve-Host bietet eine zusätzliche Redundanzebene, die für unternehmenskritische Workloads von entscheidender Bedeutung ist. Bei Dedicated Hosts stellt ein Reserve-Host sicher, dass Sie die Umgebung für unternehmenskritische Workloads aufrechterhalten, auch wenn ein primärer Host gewartet werden muss oder ein Problem auftritt.

Vorbereitung auf geplante Veranstaltungen und Veranstaltungen AWS **`system-maintenance instance-retirement`**

AWS plant zwei Arten von `system-maintenance` Ereignissen: Netzwerkwartung und Wartung der Stromversorgung.

- Bei der Netzwerkwartung wird die Netzwerkverbindung von geplanten Instances kurz unterbrochen. Die normale Netzwerkverbindung wird für Ihre Instance wiederhergestellt, nachdem die Wartung abgeschlossen ist.
- Bei der Stromversorgungswartung werden geplante Instances kurz in den Offlinezustand versetzt und dann neu gestartet. Wenn ein Neustart auf EC2-Bare-Metal-Instances durchgeführt wird, bleiben die Volume-Daten des Instance-Speichers nicht erhalten.

AWS plant `instance-retirement` EC2-Ereignisse, wenn eine Verschlechterung der zugrunde liegenden Hardware, die Ihre EC2-Instances hostet, festgestellt wird.

Um Fehler zu behebensystem-maintenance, ersetzen Sie den ausgefallenen Host mithilfe der Amazon EVS-Konsole oder AWS CLI des SDDC-Managers durch einen neuen Host, bevor das `instance-retirement` Wartungsereignis eintritt. Wenn Sie auf das Eintreten des Wartungsereignisses warten und ein Neustart der EC2-Instance erforderlich ist, verlieren Sie Ihre vSAN-Daten, die auf dem Instance-Speicher-Volume gespeichert sind. Die detaillierten Schritte finden Sie unter the section called “Ersetzen Sie einen Amazon EVS-Host”.

> **Important**
>
> Die EC2-Konsole sollte nicht verwendet werden, um den Status Ihrer Amazon EVS-Hosts zu verwalten, einschließlich Stopp, Start und Kündigung. Versuchen Sie nicht, die von Amazon EVS bereitgestellten EC2-Instances zu starten, zu stoppen oder zu beenden. Diese Aktion führt zu einem vSAN-Datenverlust.

Ersetzen Sie einen Amazon EVS-Host

Gehen Sie wie folgt vor, um einen Amazon EVS-Host zu ersetzen.

> **Warning**
>
> Amazon EVS-Hosts verwenden ein benutzerdefiniertes Anbieter-Add-on, um wichtige Host-Funktionen bereitzustellen. Wenn Sie Ihrer Umgebung einen Host hinzufügen, verfügt er über die neueste verfügbare Version des benutzerdefinierten Amazon EVS-Add-ons. Wenn Ihre Umgebung Hosts mit einer älteren Add-On-Version verwendet, führt das Hinzufügen eines Hosts zu Ihrem vSphere-Cluster dazu, dass die Cluster-Image-Standardisierung fehlschlägt. Schritte zur Behebung dieses Problems finden Sie unter. the section called “Beheben Sie den Fehler beim Hinzufügen eines Hosts aufgrund eines inkompatiblen Cluster-Images”

> **Warning**
>
> Wenn Sie Ihre ESX-Version nach der Bereitstellung aktualisiert haben, schlägt der SDDC-Manager möglicherweise bei der VCF-Host-Validierung im Schritt „Hosts in Betrieb nehmen“ fehl. Schritte zur Behebung dieses Problems finden Sie unter. the section called “SDDC Manager schlägt die VCF-Hostvalidierung bei der Host-Inbetriebnahme fehl”

> **Note**
>
> Stellen Sie sicher, dass Ihre Amazon EVS-Hostanzahl pro EVS-Umgebungskontingent korrekt eingestellt ist, um eine erfolgreiche Hosterstellung sicherzustellen. Die Hosterstellung schlägt fehl, wenn dieser Kontingentwert unter der Anzahl der Hosts liegt, die Sie in einer einzelnen Amazon EVS-Umgebung bereitstellen möchten. Möglicherweise müssen Sie

eine Erhöhung des Kontingents für Wartungsarbeiten beantragen, bei denen der Host ausgetauscht werden muss. Weitere Informationen finden Sie unter Servicekontingente.

Example

Amazon EVS console and SDDC Managuer UI

1. Gehen Sie zur Amazon EVS-Konsole.
2. Wählen Sie im Navigationsbereich die Option Umgebung aus.
3. Wählen Sie die Umgebung aus, die den zu ersetzenden Host enthält.
4. Wählen Sie die Registerkarte Hosts aus.
5. Wählen Sie Create hoste (Host erstellen) aus.
6. Geben Sie die Host-Details an und wählen Sie Create Host aus.
7. Um zu überprüfen, ob der Vorgang abgeschlossen ist, überprüfen Sie, ob der Hoststatus auf Erstellt geändert wurde.
8. Rufen Sie die Anmeldeinformationen für das ESX-Root-Passwort von AWS Secrets Manager ab. Weitere Informationen zum Abrufen von Geheimnissen finden Sie unter Geheimnisse aus AWS Secrets Manager abrufen im AWS Secrets Manager Manager-Benutzerhandbuch.
9. Gehen Sie zu SDDC Manager.
10. Nehmen Sie den neuen Host in SDDC Manager unter Verwendung der ESX-Root-Anmeldeinformationen in Betrieb, die Sie in einem vorherigen Schritt abgerufen haben. Weitere Informationen finden Sie in der VMware Cloud Foundation-Dokumentation unter Commission Hosts.
11. Fügen Sie den neuen Host dem Cluster hinzu. Weitere Informationen finden Sie unter Hinzufügen eines ESX-Hosts zu Ihrem vSphere-Cluster mithilfe des Schnellstart-Workflows in der vSphere-Dokumentation.
12. Nehmen Sie den alten Host in SDDC Manager außer Betrieb, den Sie aus SDDC Manager entfernen möchten. Weitere Informationen finden Sie in der Cloud Foundation-Dokumentation unter Außerbetriebnahme von Hosts. VMware
13. Kehren Sie zur Amazon EVS-Konsole zurück.
14. Wählen Sie auf der Registerkarte Hosts den ausgefallenen Host aus und wählen Sie Löschen > Host löschen.

AWS CLI and SDDC Manager UI

1. Öffnen Sie eine neue Terminalsitzung.
2. Erstellen Sie einen neuen Host. Im Folgenden finden Sie einen Beispielbefehl als Referenz.

```
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. Rufen Sie die Anmeldeinformationen für das ESX-Root-Passwort von AWS Secrets Manager ab. Weitere Informationen zum Abrufen von Geheimnissen finden Sie unter Geheimnisse aus AWS Secrets Manager abrufen im AWS Secrets Manager Manager-Benutzerhandbuch.
4. Gehen Sie zu SDDC Manager.
5. Nehmen Sie den neuen Host in SDDC Manager unter Verwendung der ESX-Root-Anmeldeinformationen in Betrieb, die Sie in einem vorherigen Schritt abgerufen haben. Weitere Informationen finden Sie in der VMware Cloud Foundation-Dokumentation unter Commission Hosts.
6. Fügen Sie den neuen Host dem Cluster hinzu, der den beeinträchtigten Host enthält.
7. Nehmen Sie den beeinträchtigten Host im SDDC Manager außer Betrieb. Weitere Informationen finden Sie in der Cloud Foundation-Dokumentation unter Außerbetriebnahme von Hosts. VMware
8. Kehren Sie zum Terminal zurück.
9. Löscht den ausgefallenen Host. Im Folgenden finden Sie einen Beispielbefehl als Referenz.

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

Fehlerbehebung

Hinweise zu Broadcom und AWS Support

AWS bietet Unterstützung für Amazon EVS und die zugehörigen Infrastrukturdienste, einschließlich VMware Cloud Foundation (VCF). Für VCF-spezifische Konfigurationsanleitungen oder Probleme im

Zusammenhang mit anderen VMware Produkten wie Aria Suite, HCX oder NSX können Sie sich mit Ihrem Broadcom-Supportanspruch auch direkt an Broadcom wenden. Weitere Informationen finden Sie im Broadcom Support Portal.

Anleitungen zur Fehlerbehebung finden Sie unterFehlerbehebung. Wenn Sie nach dem Lesen der Anleitung zur Fehlerbehebung weiterhin Probleme haben, wenden Sie sich an den AWS Support, um weitere Unterstützung zu erhalten.

Konfigurieren Sie eine benutzerdefinierte Routing-Tabelle für Amazon EVS-Subnetze

Amazon EVS unterstützt die Verwendung einer benutzerdefinierten Routentabelle erst, nachdem die Amazon EVS-Umgebung erstellt wurde. Um eine erfolgreiche Umgebungserstellung zu ermöglichen, müssen Sie die Haupt-Routing-Tabelle so konfigurieren, dass Datenverkehr zu abhängigen Diensten wie DNS und lokalen Systemen zugelassen wird. Dies liegt daran, dass Amazon EVS-VLAN-Subnetze während der Bereitstellung der Umgebung implizit mit der Haupt-Routing-Tabelle unserer VPC verknüpft werden.

Nach der Bereitstellung Ihrer Umgebung müssen Sie jedes der Amazon EVS-VLAN-Subnetze explizit einer Routing-Tabelle in Ihrer VPC zuordnen. Die NSX-Konnektivität schlägt fehl, wenn Ihre VLAN-Subnetze nicht explizit einer VPC-Routentabelle zugeordnet sind. Wir empfehlen dringend, dass Sie Ihre Subnetze explizit einer benutzerdefinierten Routentabelle zuordnen. Eine benutzerdefinierte Routingtabelle bietet eine detailliertere Kontrolle über das Routing des Netzwerkverkehrs innerhalb Ihrer VPC und ermöglicht maßgeschneiderte Routing-Regeln für bestimmte Subnetze oder Gateways. Weitere Informationen zum Erstellen einer benutzerdefinierten Routentabelle finden Sie unter Erstellen einer Routentabelle für Ihre VPC im Amazon VPC-Benutzerhandbuch.

Konfiguration einer Netzwerkzugriffskontrollliste zur Steuerung des Amazon EVS-VLAN-Subnetzverkehrs

Eine Netzwerk-Zugriffssteuerungsliste (ACL) erlaubt oder verweigert bestimmten eingehenden oder ausgehenden Datenverkehr auf der Subnetzebene. Sie können das Netzwerk verwenden ACLs , um den eingehenden und ausgehenden Verkehr für Ihre Amazon EVS-VLAN-Subnetze zu kontrollieren. Weitere Informationen finden Sie unter Erstellen einer Netzwerk-ACL für Ihre VPC im Amazon VPC-Benutzerhandbuch.

Important

EC2 Sicherheitsgruppen funktionieren nicht auf elastischen Netzwerkschnittstellen, die mit Amazon EVS-VLAN-Subnetzen verbunden sind. Um den Verkehr zu und von Amazon EVS VLAN-Subnetzen zu kontrollieren, müssen Sie eine Netzwerkzugriffskontrollliste verwenden.

Warning

Amazon EVS benötigt Zugriff auf Ihre VCF-Bereitstellung. Sie müssen Ihre Sicherheitsgruppen und Netzwerkzugriffskontrolllisten (ACLs) konfigurieren, damit Amazon EVS kommunizieren kann mit:

- DNS-Server über TCP/UDP Port 53.
- Host-Management-VLAN-Subnetz über HTTPS und SSH.
- VLAN-Subnetz der Verwaltungs-VM über HTTPS und SSH.

Wenn Ihre Sicherheitsgruppen und Ihr Netzwerk diesen Zugriff ACLs nicht zulassen, schlägt die Bereitstellung der Amazon EVS-Umgebung fehl und bestehende Umgebungen weisen möglicherweise einen eingeschränkten Compliance-Status auf.

Geheimer Verwaltungslebenszyklus

Amazon EVS verwendet AWS Secrets Manager, um Geheimnisse bei der ersten Bereitstellung der Umgebung in Ihrem Konto zu erstellen, zu verschlüsseln und zu speichern. Diese Geheimnisse enthalten die VCF-Anmeldeinformationen, die für die Installation und den Zugriff auf VCF-Verwaltungs-Appliances wie vCenter Server, NSX und SDDC Manager erforderlich sind, sowie das ESX-Host-Root-Passwort. Amazon EVS löscht auch verwaltete Geheimnisse in Ihrem Namen, wenn die EVS-Umgebung gelöscht wird.

Sie sind verantwortlich für die Verwaltung des geheimen Lebenszyklus, einschließlich der geheimen Rotation. Amazon EVS bietet keine verwaltete Rotation Ihrer Secrets. Wir empfehlen, dass Sie die Geheimnisse regelmäßig innerhalb eines festgelegten Rotationsfensters wechseln, um sicherzustellen, dass Geheimnisse nicht langlebig sind. Weitere Informationen finden Sie unter Rotationspläne im AWS Secrets Manager Manager-Benutzerhandbuch.

Erstellen Sie einen Amazon EVS-Host

Nach der Bereitstellung einer Amazon EVS-Umgebung können Sie Hosts hinzufügen, um die Kapazität und Workload-Resilienz zu erhöhen. Amazon EVS unterstützt 4-16 Hosts pro Umgebung. Diese Aktion kann erst verwendet werden, nachdem die Amazon EVS-Umgebung bereitgestellt wurde.

> **Note**
>
> Sie müssen den Host über die SDDC Manager-Benutzeroberfläche zuweisen und in Betrieb nehmen.

So erstellen Sie einen Amazon EVS-Host

Gehen Sie wie folgt vor, um einen Amazon EVS-Host zu erstellen.

> **Warning**
>
> Amazon EVS-Hosts verwenden ein benutzerdefiniertes Anbieter-Add-on, um wichtige Host-Funktionen bereitzustellen. Wenn Sie Ihrer Umgebung einen Host hinzufügen, verfügt er über die neueste verfügbare Version des benutzerdefinierten Amazon EVS-Add-ons. Wenn Ihre Umgebung Hosts mit einer älteren Add-On-Version verwendet, führt das Hinzufügen eines Hosts zu Ihrem vSphere-Cluster dazu, dass die Cluster-Image-Standardisierung fehlschlägt. Schritte zur Behebung dieses Problems finden Sie unter. the section called “Beheben Sie den Fehler beim Hinzufügen eines Hosts aufgrund eines inkompatiblen Cluster-Images”

> **Warning**
>
> Wenn Sie Ihre ESX-Version nach der Bereitstellung der Amazon EVS-Umgebung aktualisiert haben, schlägt der SDDC-Manager möglicherweise bei der VCF-Host-Validierung im Schritt Provision-Hosts fehl. Schritte zur Behebung dieses Problems finden Sie unter. the section called “SDDC Manager schlägt die VCF-Hostvalidierung bei der Host-Inbetriebnahme fehl”

> **Note**
>
> Stellen Sie sicher, dass Ihre Amazon EVS-Hostanzahl pro EVS-Umgebungskontingent korrekt eingestellt ist, um eine erfolgreiche Hosterstellung sicherzustellen. Die Hosterstellung schlägt fehl, wenn dieser Kontingentwert unter der Anzahl der Hosts liegt, die Sie in einer einzelnen Amazon EVS-Umgebung bereitstellen möchten. Um das Kontingent zu erhöhen, können Sie eine Erhöhung des Kontingents beantragen. Weitere Informationen finden Sie unter Servicekontingente.

> **Note**
>
> Wenn Sie beim Hinzufügen von Hosts zu Ihrer Umgebung keine ESX-Version angeben, verwendet Amazon EVS automatisch die ESX-Standardversion, die der VCF-Version Ihrer Umgebung zugeordnet ist. Weitere Informationen finden Sie unter the section called “VCF-Versionen und EC2-Instances”.

> **Important**
>
> Wählen Sie beim Hinzufügen eines ESX-Hosts eine ESX-Version aus, die Ihrem vSphere-Zielcluster entspricht. Wenn dieselbe Version nicht verfügbar ist, stellen Sie eine ältere Version bereit und führen Sie ein Upgrade mit vSphere Lifecycle Manager durch. Weitere Informationen finden Sie unter the section called “SDDC Manager schlägt die VCF-Hostvalidierung bei der Host-Inbetriebnahme fehl”. Upgrades erfordern möglicherweise einen Neustart des Hosts und verlängern die Zeit, die für die Inbetriebnahme des Hosts benötigt wird.
>
> Ein Host mit einer ESX-Version, die neuer ist als die ESX-Version Ihres vSphere-Cluster-Images, kann nicht herabgestuft werden. Sie müssen den Host löschen und ihn mit der richtigen ESX-Version neu erstellen.

Example

Amazon EVS console and SDDC Managuer UI

1. Gehen Sie zur Amazon EVS-Konsole.

2. Wählen Sie im Navigationsbereich die Option Umgebung aus.
3. Wählen Sie die Umgebung aus, in der Sie den Host erstellen möchten.
4. Wählen Sie die Registerkarte Hosts aus.
5. Wählen Sie Create hoste (Host erstellen) aus.
6. Geben Sie die Host-Details an und wählen Sie Create Host aus.
7. Um den Abschluss zu überprüfen, überprüfen Sie, ob der Hoststatus auf Erstellt geändert wurde.
8. Gehen Sie zu SDDC Manager.
9. Nehmen Sie den neuen Host in SDDC Manager in Betrieb. Weitere Informationen finden Sie in der VMware Cloud Foundation-Dokumentation unter Commission Hosts.
10. Fügen Sie den neuen Host mithilfe von SDDC Manager zum Cluster hinzu. Weitere Informationen finden Sie unter Hinzufügen eines ESX-Hosts zu Ihrem vSphere-Cluster mithilfe des Schnellstart-Workflows in der vSphere-Dokumentation.

AWS CLI and SDDC Manager UI

1. Öffnen Sie eine neue Terminalsitzung.
2. Erstellen Sie einen neuen Host. Im Folgenden finden Sie einen Beispielbefehl als Referenz.

```
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. Gehen Sie zum SDDC-Manager.
4. Nehmen Sie den neuen Host in SDDC Manager in Betrieb. Weitere Informationen finden Sie in der VMware Cloud Foundation-Dokumentation unter Commission Hosts.
5. Fügen Sie den neuen Host mithilfe von SDDC Manager zum Cluster hinzu. Weitere Informationen finden Sie unter Hinzufügen eines ESX-Hosts zu Ihrem vSphere-Cluster mithilfe des Schnellstart-Workflows in der vSphere-Dokumentation.

Löschen Sie einen Amazon EVS-Host

Sie können einen Amazon EVS-Host aus Ihrer Umgebung löschen, wenn der Host nicht mehr benötigt wird. Amazon EVS setzt voraus, dass Ihre Umgebung über mindestens vier Hosts verfügt. Amazon EVS unterstützt keine Umgebungen mit weniger als vier Hosts.

> **Warning**
>
> Wenn Sie einen Host ohne Außerbetriebnahme löschen, bleiben veraltete Daten in Ihrem vCenter und SDDC Manager zurück, deren Bereinigung möglicherweise zusätzlichen Aufwand erfordert. Stellen Sie sicher, dass Ihre Hosts außer Betrieb genommen wurden, bevor Sie Hosts in der Amazon EVS-Konsole oder API löschen.

> **Warning**
>
> Verwenden Sie immer die Amazon EVS-Konsole oder API, um Ihre Amazon EVS-Hosts zu entfernen. Das Löschen von Hosts aus der EC2 Konsole kann dazu führen, dass Ihre Umgebung in einem inkonsistenten Zustand bleibt.

So löschen Sie einen Amazon EVS-Host

Gehen Sie wie folgt vor, um einen Amazon EVS-Host zu löschen.

Example

SDDC Managuer UI and Amazon EVS console

1. Gehen Sie zum SDDC Manager.
2. Entfernen Sie den Cluster aus dem SDDC Manager.
3. Nehmen Sie den Host im SDDC Manager außer Betrieb. Weitere Informationen finden Sie in der Cloud Foundation-Dokumentation unter Außerbetriebnahme von Hosts. VMware
4. Gehen Sie zur Amazon EVS-Konsole.
5. Wählen Sie im Navigationsbereich Umgebung aus.
6. Wählen Sie die Umgebung aus, die den zu löschenden Host enthält.
7. Wählen Sie die Registerkarte Hosts aus.

8. Wählen Sie Host löschen.
9. Wählen Sie den Host aus und klicken Sie auf der Registerkarte Hosts auf Löschen. Wiederholen Sie diesen Schritt für jeden Host, den Sie löschen möchten.

SDDC Manager UI and AWS CLI

1. Gehen Sie zu SDDC Manager.
2. Entfernen Sie den Cluster aus dem SDDC Manager.
3. Nehmen Sie den Host im SDDC Manager außer Betrieb. Weitere Informationen finden Sie in der Cloud Foundation-Dokumentation unter Außerbetriebnahme von Hosts. VMware
4. Öffnen Sie eine neue Terminalsitzung.
5. Löschen Sie den Host. Im Folgenden finden Sie einen Beispielbefehl als Referenz.

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

Erstellen Sie einen Amazon EVS-Umgebungskonnektor

Sie können einen Connector erstellen, damit Amazon EVS mit einer VCF-Verwaltungs-Appliance wie vCenter Server in Ihrer Umgebung kommunizieren kann. Ein Connector verwendet den vollqualifizierten Domänennamen (FQDN) für die Appliance und Anmeldeinformationen, die Sie in einem AWS Secrets Manager Manager-Geheimnis speichern, um sich bei der Appliance zu authentifizieren.

Weitere Informationen zu Konnektoren finden Sie unter Konzepte und Komponenten von Amazon EVS.

> **Warning**
>
> Bevor Sie einen Connector erstellen, empfehlen wir Ihnen, einen dedizierten vCenter-Benutzer mit einer ReadOnly Rolle zu erstellen. Vermeiden Sie es, Anmeldeinformationen mit erhöhten Rechten oder Administratorrechten zu verwenden.

> **Note**
>
> Bevor Sie einen Connector erstellen, müssen Sie in AWS Secrets Manager ein Geheimnis mit Ihren Appliance-Anmeldeinformationen erstellen. Das Geheimnis muss zwei Schlüssel `username` und enthaltenpassword. Bei den Werten muss es sich um die Anmeldeinformationen für den dedizierten Benutzer handeln, den Sie für die im Connector angegebene Appliance erstellt haben.

> **Important**
>
> Sie müssen das Tag `EvsAccess=true` zu Ihrem Secrets Manager Manager-Geheimnis hinzufügen. Wenn Sie das Geheimnis mit Ihrem eigenen verschlüsselt haben AWS KMS key, fügen Sie das `EvsAccess=true` Tag AWS KMS key auch dem hinzu.

> **Note**
>
> Jeder Connector ist einem einzelnen FQDN der Appliance zugeordnet.

> **Note**
>
> Pro Umgebung ist nur ein Connector vom Typ vCenter zulässig.

> **Note**
>
> Der FQDN muss gültig sein, mit dem Domänennamen übereinstimmen, der bei der Erstellung Ihrer EVS-Umgebung verwendet wurde, und für alle Konnektoren in der Umgebung eindeutig sein.

> **Note**
>
> Durch die Erstellung des Connectors werden weder die Erreichbarkeit noch die Anmeldeinformationen der Appliance überprüft. Wenn der Connector den Status Aktiv

hat, wird der Status der Erreichbarkeitsprüfung innerhalb von 10 Minuten asynchron von Unbekannt auf Bestanden oder Fehlgeschlagen aktualisiert.

So erstellen Sie einen Amazon EVS-Umgebungsconnector

Gehen Sie wie folgt vor, um einen Amazon EVS-Connector zu erstellen.

Example

Amazon EVS console

1. Gehen Sie zur Amazon EVS-Konsole.
2. Wählen Sie im Navigationsbereich Environments (Umgebungen) aus.
3. Wählen Sie die Umgebung aus, in der Sie den Connector erstellen möchten.
4. Wählen Sie die Registerkarte Konnektoren aus.
5. Wählen Sie Konnektor erstellen.
6. Geben Sie für Appliance-FQDN den vollqualifizierten Domänennamen der Appliance ein.
7. Wählen Sie in der Dropdownliste Secrets Manager das Secret aus, das die Anmeldeinformationen der Appliance enthält.
8. Wählen Sie Konnektor erstellen.
9. Um den Abschluss zu überprüfen, überprüfen Sie, ob der Connector-Status Aktiv und das Ergebnis der Erreichbarkeitsprüfung „Bestanden“ lautet.

AWS CLI

1. Öffnen Sie eine neue Terminalsitzung.
2. Erstellen Sie einen neuen Connector. Im Folgenden finden Sie einen Beispielbefehl als Referenz.
   - secret-identifier kann der geheime Name oder der ARN sein

```
aws evs create-environment-connector \
    --environment-id env-abcde12345 \
    --type VCENTER \
    --appliance-fqdn vcenter.example.com \
    --secret-identifier arn:aws:secretsmanager:us-
east-2:123456789012:secret:vcenter-creds-AbCdEf
```

3. Um den Abschluss zu überprüfen, verwenden Sie den list-environment-connectorsBefehl und überprüfen Sie, ob der Connector-Status Aktiv und das Ergebnis der Erreichbarkeitsprüfung Bestanden lautet.

```
aws evs list-environment-connectors \
    --environment-id env-abcde12345
```

Aktualisieren Sie einen Amazon EVS-Umgebungsconnector

Sie können einen vorhandenen Connector aktualisieren, um den FQDN der Appliance zu ändern, oder zur Authentifizierung auf ein anderes Secrets Manager Manager-Geheimnis verweisen. Beispielsweise müssen Sie möglicherweise den FQDN aktualisieren, wenn sich der Endpunkt der Appliance ändert, oder zu einem anderen Secret wechseln. Sie können die Werte des vorhandenen Secrets Manager Manager-Geheimnisses auch direkt aktualisieren, wenn Sie die vCenter-Anmeldeinformationen rotieren, sodass kein Connector-Update erforderlich ist.

Weitere Informationen zu Konnektoren finden Sie unter Konzepte und Komponenten von Amazon EVS.

> **Note**
>
> Es kann jeweils nur eine Eigenschaft eines Connectors aktualisiert werden.

> **Note**
>
> Der Connector muss den Status Aktiv oder Aktualisierung fehlgeschlagen haben, um aktualisiert zu werden.

> **Note**
>
> Wenn Sie den FQDN aktualisieren, muss der neue FQDN gültig sein, mit dem Domänennamen übereinstimmen, der bei der Erstellung Ihrer EVS-Umgebung verwendet wurde, und für alle Konnektoren in der Umgebung eindeutig sein.

So aktualisieren Sie einen Amazon EVS-Umgebungsconnector

Gehen Sie wie folgt vor, um einen Amazon EVS-Connector zu aktualisieren.

Example

Amazon EVS console

1. Gehen Sie zur Amazon EVS-Konsole.
2. Wählen Sie im Navigationsbereich Environments (Umgebungen) aus.
3. Wählen Sie die Umgebung aus, die den Connector enthält.
4. Wählen Sie die Registerkarte Konnektoren aus.
5. Wählen Sie den Connector aus, den Sie aktualisieren möchten.
6. Wählen Sie Aktionen und dann in der Dropdownliste die Option Geheimes Update oder FQDN aktualisieren aus.
7. Für Update Secret:
   a. Wählen Sie in der Dropdownliste „Secret“ das Secret mit den Anmeldeinformationen der Appliance aus und wählen Sie „Aktualisieren“.
8. Für Update FQDN:
   a. Geben Sie den neuen FQDN ein und wählen Sie Update.
9. Um den Abschluss zu überprüfen, überprüfen Sie, ob der Connector-Status nach dem Update wieder auf Aktiv zurückgesetzt wurde.

AWS CLI

1. Öffnen Sie eine neue Terminalsitzung.
2. Aktualisieren Sie den geheimen Konnektorschlüssel oder den FQDN. Nachfolgend finden Sie Beispielbefehle als Referenz.

   Um das Geheimnis zu aktualisieren:

```
aws evs update-environment-connector \
    --environment-id env-abcde12345 \
    --connector-id cnctr-szgj87q6gi \
    --secret-identifier arn:aws:secretsmanager:us-
east-2:123456789012:secret:vcenter-creds-AbCdEf
```

Um den FQDN zu aktualisieren:

```
aws evs update-environment-connector \
    --environment-id env-abcde12345 \
    --connector-id cnctr-szgj87q6gi \
    --appliance-fqdn vcf.evs.dev
```

3. Um den Abschluss zu überprüfen, verwenden Sie den list-environment-connectorsBefehl und überprüfen Sie, ob der Connector-Status Aktiv ist.

```
aws evs list-environment-connectors \
    --environment-id env-abcde12345
```

Löschen Sie einen Amazon EVS-Umgebungsconnector

Sie können einen Connector löschen, wenn er nicht mehr benötigt wird.

Weitere Informationen zu Konnektoren finden Sie unter Konzepte und Komponenten von Amazon EVS.

> **Note**
>
> Der Connector muss den Status Aktiv, Erstellung fehlgeschlagen oder Aktualisierung fehlgeschlagen haben, um gelöscht zu werden.

> **Note**
>
> Alle mit dem Connector verknüpften Berechtigungen müssen gelöscht werden, bevor der Connector entfernt werden kann.

So löschen Sie einen Amazon EVS-Umgebungsconnector

Gehen Sie wie folgt vor, um einen Amazon EVS-Connector zu löschen.

Example

Amazon EVS console

1. Gehen Sie zur Amazon EVS-Konsole.
2. Wählen Sie im Navigationsbereich Environments (Umgebungen) aus.
3. Wählen Sie die Umgebung aus, die den Connector enthält.
4. Wählen Sie die Registerkarte Konnektoren aus.
5. Wählen Sie den Connector aus, den Sie löschen möchten.
6. Wählen Sie Connector löschen.
7. Bestätigen Sie das Löschen.
8. Um den Abschluss zu überprüfen, stellen Sie sicher, dass der Connector nicht mehr in der Liste erscheint.

AWS CLI

1. Öffnen Sie eine neue Terminalsitzung.
2. Löschen Sie den Connector. Im Folgenden finden Sie einen Beispielbefehl als Referenz.

```
aws evs delete-environment-connector \
    --environment-id env-abcde12345 \
    --connector-id cnctr-szgj87q6gi
```

3. Um den Abschluss zu überprüfen, verwenden Sie den list-environment-connectorsBefehl und vergewissern Sie sich, dass der Connector nicht mehr aufgeführt ist.

```
aws evs list-environment-connectors \
    --environment-id env-abcde12345
```

Erstellen Sie eine Amazon EVS-Berechtigung

Sie können Windows Server-Berechtigungen für eine oder mehrere virtuelle Maschinen (VMs) erstellen, die in Ihrer Amazon EVS-Umgebung ausgeführt werden. Nachdem Sie eine Berechtigung erstellt haben und die VM eingeschaltet ist, beginnt Amazon EVS mit der Überwachung der Windows Server-Berechtigungsnutzung der entsprechenden VM, sodass Sie Windows Server-Lizenzen direkt AWS auf Basis nutzen können. pay-as-you-go

Weitere Informationen zu Berechtigungen finden Sie unter Konzepte und Komponenten von Amazon EVS.

> **Note**
>
> Es können nur 100 Berechtigungen gleichzeitig erstellt werden.

> **Note**
>
> Sie müssen einen vCenter-Connector erstellen, bevor Sie Berechtigungen erstellen können. Der Connector muss sich im Status Aktiv befinden und die Erreichbarkeitsprüfung muss sich im Status „Bestanden“ befinden.

> **Note**
>
> Die Validierung erfolgt asynchron. Wenn die Validierung einer VM fehlschlägt (z. B. weil das Gastbetriebssystem nicht unterstützt wird oder die VM nicht gefunden wurde), wird ihr Berechtigungsstatus auf „Erstellen fehlgeschlagen mit Fehlerdetails“ gesetzt. Sie können das zugrunde liegende Problem beheben und dann die Berechtigung erneut erstellen.

> **Note**
>
> In vCenter können Sie PowerCLI oder andere Tools verwenden, um die VM Managed Object ID abzurufen.

So erstellen Sie eine Amazon EVS-Berechtigung

Gehen Sie wie folgt vor, um eine Amazon EVS-Berechtigung zu erstellen.

Example

Amazon EVS console

1. Gehen Sie zur Amazon EVS-Konsole.

2. Wählen Sie im Navigationsbereich Environments (Umgebungen) aus.
3. Wählen Sie die Umgebung aus, die die VMs enthält.
4. Wählen Sie die Registerkarte Berechtigungen aus.
5. Wählen Sie Hinzufügen aus.
6. Der Produkttyp ist standardmäßig Windows Server.
7. Fügen VMs Sie die Elemente, für die Sie Berechtigungen erstellen möchten, per Text oder durch Hochladen einer CSV-Datei hinzu.
   - Das CSV-Format ist eine einzelne Spalte, die nur VM enthält. IDs
8. Wählen Sie Anspruch hinzufügen aus.
9. Um den Abschluss zu überprüfen, überprüfen Sie, ob der Anspruchsstatus auf Erstellt geändert wurde.

AWS CLI

1. Öffnen Sie eine neue Terminalsitzung.
2. Erstellen Sie Berechtigungen. Im Folgenden finden Sie einen Beispielbefehl als Referenz.

```
aws evs create-entitlement \
    --environment-id env-abcde12345 \
    --connector-id cnctr-szgj87q6gi \
    --entitlement-type WINDOWS_SERVER \
    --vm-ids vm-001 vm-002 vm-003
```

3. Um den Abschluss zu überprüfen, listen Sie die VM-Berechtigungen auf und überprüfen Sie, ob der Berechtigungsstatus Erstellt lautet.

```
aws evs list-vm-entitlements \
  --environment-id env-abcde12345 \
  --connector-id cnctr-szgj87q6gi \
  --entitlement-type WINDOWS_SERVER
```

Löschen Sie eine Amazon EVS-Berechtigung

Sie können Windows Server-Berechtigungen für eine oder mehrere virtuelle Maschinen (VMs) in Ihrer Amazon EVS-Umgebung löschen. Wenn Sie eine Berechtigung löschen, hört Amazon EVS auf,

die Nutzung der Windows Server-Berechtigungen für die angegebene VM zu verfolgen. Nach dem Löschen hat die VM keine Windows Server-Berechtigung mehr. AWS

Weitere Informationen zu Berechtigungen finden Sie unter Konzepte und Komponenten von Amazon EVS.

> **Note**
>
> Sie können jeweils nur bis zu 100 Berechtigungen löschen.

> **Note**
>
> Sie müssen die VM angeben IDs , von der Berechtigungen gelöscht werden sollen.

> **Note**
>
> Nach dem Löschen haben VMs sie keine Windows Server-Berechtigungen mehr. AWS

So löschen Sie eine Amazon EVS-Berechtigung

Gehen Sie wie folgt vor, um eine Amazon EVS-Berechtigung zu löschen.

Example

Amazon EVS console

1. Gehen Sie zur Amazon EVS-Konsole.
2. Wählen Sie im Navigationsbereich Environments (Umgebungen) aus.
3. Wählen Sie die Umgebung aus, die die VMs enthält.
4. Wählen Sie die Registerkarte Berechtigungen aus.
5. Wählen VMs Sie die aus, für die Sie Berechtigungen löschen möchten.
6. Wählen Sie Löschen aus.
7. Bestätigen Sie das Entfernen.
8. Um zu überprüfen, ob der Vorgang abgeschlossen ist, überprüfen Sie, ob die jeweiligen VMs Berechtigungen aus der Konsolenliste entfernt wurden.

AWS CLI

1. Öffnen Sie eine neue Terminalsitzung.
2. Löscht eine Berechtigung. Im Folgenden finden Sie einen Beispielbefehl als Referenz.

```
aws evs delete-entitlement \
    --environment-id env-abcde12345 \
    --connector-id cnctr-szgj87q6gi \
    --entitlement-type WINDOWS_SERVER \
    --vm-ids vm-003 vm-001
```

3. Um den Abschluss zu überprüfen, listen Sie die Berechtigungen auf und vergewissern Sie sich, dass die gelöschten Berechtigungen nicht mehr vorhanden VMs sind.

```
aws evs list-vm-entitlements \
    --environment-id env-abcde12345 \
    --connector-id cnctr-szgj87q6gi \
    --entitlement-type WINDOWS_SERVER
```

Windows Server-Aktivierung konfigurieren

Amazon EVS bietet Windows Server-Aktivierung für Personen VMs mit Windows Server-Berechtigungen. Sie müssen einen VPC-Endpunkt zur Aktivierung von EVS Windows Server innerhalb der VPC erstellen, die Sie für Ihre Amazon EVS-Umgebung verwendet haben.
Jede berechtigte VM muss dann so konfiguriert werden, dass sie eine Verbindung zu diesem Aktivierungsendpunkt herstellt. VPC-Endpoints können nur erstellt werden, wenn Sie über eine aktive Amazon EVS-Umgebung verfügen.

1. Identifizieren Sie die VPC, in der die Amazon EVS-Umgebung bereitgestellt wird.
2. Erstellen Sie in derselben VPC einen VPC-Endpunkt mit dem folgenden Dienstnamen:

   `com.amazonaws.<region>.evs-windows-server-activation`

   Erstellen Sie beispielsweise einen VPC-Endpunkt mit der folgenden Konfiguration:

   - Typ: Dienste AWS
   - Dienstname: suchen und auswählen `com.amazonaws.<region>.evs-windows-server-activation`
   - VPC: Wählen Sie die VPC aus, in der sich Ihre Amazon EVS-Umgebung befindet

- Subnetze: Wählen Sie die Subnetze aus, aus denen Ihr Windows ausgehende Verbindungen herstellt VMs
- Sicherheitsgruppen: Wählen oder erstellen Sie eine, die eingehende TCP-Ports 1688 aus der Sicherheitsgruppe/CIDR Ihrer Windows-Instanz zulässt

3. Notieren Sie sich den privaten DNS-Namen des VPC-Endpunkts, den Sie erstellt haben.
4. Connect zur Windows Server-VM her und öffnen Sie PowerShell.
5. Konfigurieren Sie den Aktivierungsserver für die Verwendung des VPC-Endpunkts mit dem folgenden Befehl:

   ```
   slmgr /skms <VPC Endpoint Private DNS Name>:1688
   ```

   Sie erhalten ein Dialogfeld, in dem bestätigt wird, dass der Aktivierungsserver eingerichtet wurde.
6. Aktivieren Sie Windows Server mit dem folgenden Befehl:

   ```
   slmgr /ato
   ```

   Es sollte ein Dialogfeld mit der Meldung "Das Produkt wurde erfolgreich aktiviert“ angezeigt werden. “
7. Überprüfen Sie mit dem folgenden Befehl, ob die Aktivierung erfolgreich abgeschlossen wurde:

   ```
   slmgr /dli
   ```

   Suchen Sie nach Lizenzstatus: Lizenziert.

Sicherheit in Amazon Elastic VMware Service

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Im Modell der übergreifenden Verantwortlichkeit wird Folgendes mit „Sicherheit der Cloud“ bzw. „Sicherheit in der Cloud“ umschrieben:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS-Services in der läuft AWS Cloud. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der AWS -Compliance-Programme regelmäßig. Weitere Informationen zu den Compliance-Programmen, die für Amazon Elastic VMware Service (Amazon EVS) gelten, finden Sie AWS-Services unter Umfang nach Compliance-Programmen.
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS-Service , was Sie verwenden. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung von Amazon EVS anwenden können. Es zeigt Ihnen, wie Sie Amazon EVS konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere verwenden können AWS-Services , die Ihnen helfen, Ihre Amazon EVS-Ressourcen zu überwachen und zu sichern.

Inhalt

Datenschutz in Amazon EVS

Das Modell der AWS gemeinsamen Verantwortung gilt für den Datenschutz in Amazon Elastic VMware Service. AWS Ist, wie in diesem Modell beschrieben, für den Schutz der globalen

Infrastruktur verantwortlich, auf der die gesamte AWS Cloud läuft. Sie sind dafür verantwortlich, die Kontrolle über Ihre Inhalte zu behalten, die auf dieser Infrastruktur gehostet werden, einschließlich der VMware Cloud Foundation (VCF) -Komponenten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben der von Ihnen verwendeten AWS-Services Geräte verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen über den Datenschutz in Europa finden Sie im Blog-Beitrag AWS Modell der geteilten Verantwortlichkeit und die DSGVO im Blog zur -Sicherheit AWS .

Aus Datenschutzgründen empfehlen wir, dass Sie Ihre AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder einrichten AWS Identity and Access Management. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Wird verwendet SSL/TLS , um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein AWS CloudTrail. Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.

  > **Note**
  >
  > Amazon EVS protokolliert keine Benutzeraktivitäten für AWS Nichtkomponenten, wie z. B. Aktivitäten in Ihrer VCF-Umgebung. Diese Aktivitäten werden in verschiedenen VMware Konsolen wie vSphere und NSX Manager protokolliert. Wenn eine zentralisierte VCF-Protokollierung gewünscht wird, können Sie VCF-Überwachungslösungen wie VMware Aria Operations oder VMware Tanzu Observability konfigurieren, um dieses Ergebnis zu erzielen. Weitere Informationen finden Sie in der VMware VCF-Dokumentation unter Cloud Foundation mit VMware Tanzu und VMware Aria Suite Lifecyle im VMware Cloud Foundation-Modus.

- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen. AWS-Services
- Verwenden Sie erweiterte verwaltete Sicherheitsdienste wie Amazon Macie, die Sie bei der Erkennung und Sicherung sensibler Daten unterstützen, die in gespeichert sind Amazon S3.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere

Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

Wir empfehlen dringend, dass Sie niemals vertrauliche Informationen, wie z. B. die E-Mail-Adressen Ihrer Kunden, in Tags oder frei formatierte Textfelder wie ein Namensfeld eingeben. Dies gilt auch, wenn Sie mit Amazon EVS oder anderen AWS-Services über die Konsole AWS CLI, API oder AWS SDKs arbeiten. Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Verschlüsselung im Ruhezustand

Amazon EVS stellt EC2-Metal-Instances bereit, die standardmäßig eine transparente AES-256-Verschlüsselung für Daten verwenden, die auf dem Instance-Speicher-Volume gespeichert sind. Amazon EVS unterstützt derzeit keine Verschlüsselung des EBS-Startvolumens.

Amazon EBS-Startvolume

Amazon EVS-Instances verwenden ein Amazon EBS-Startvolume. Das Startvolume enthält das Betriebssystem und andere Dateien, die für den Start und die Ausführung der EC2-Instance erforderlich sind. Das Startvolume ist nicht verschlüsselt. Amazon EVS unterstützt derzeit keine Verschlüsselung von Startvolumes. Das Startvolume enthält keine Benutzerdaten von Ihren virtuellen Maschinen.

Instance-Speicher-Volume

Amazon EVS EC2 Metal-Instances verfügen über lokalen NVMe SSD-Speicher, der Teil der Hardware der Instance ist. Amazon EVS verwendet NVMe Instance-Speicher-Volumes als Festplatten für vSAN-Datenspeicher. Der vSAN-Datenspeicher enthält Ihre virtuellen Management- und Workload-Maschinen, nachdem Sie Ihre Amazon EVS-Umgebung bereitgestellt haben.

Die Daten auf NVMe Instance-Speicher-Volumes werden mit einer XTS-AES-256-Verschlüsselung verschlüsselt, die auf einem Hardwaremodul auf der Instance implementiert ist. Die Schlüssel, die zur Verschlüsselung von Daten verwendet werden, die auf lokal angeschlossene NVMe Speichergeräte geschrieben werden, werden pro Kunde und pro Volume vergeben. Weitere Informationen finden Sie unter Verschlüsselung im Ruhezustand im Amazon EC2 EC2-Benutzerhandbuch.

Nach der Bereitstellung der Amazon EVS-Umgebung können Sie die data-at-rest vSAN-Verschlüsselung für alle im vSAN-Datenspeicher gespeicherten Daten, für einzelne virtuelle Maschinen (VMs) oder für einzelne Dateien darin aktivieren. VMs Diese detaillierte Steuerung kann nützlich sein, wenn einige verschlüsselt werden VMs müssen und andere nicht, oder wenn bestimmte Festplatten oder Dateien innerhalb einer VM verschlüsselt werden müssen. Weitere Informationen finden Sie unter So funktioniert die Data-At-Rest vSAN-Verschlüsselung in der VMware vSAN-Dokumentation.

Verschlüsselung während der Übertragung

Amazon EVS verschlüsselt Ihren während der Übertragung befindlichen Verkehr standardmäßig nicht. Um die Daten zu verschlüsseln, die Amazon EVS übertragen, können Sie die Verschlüsselung auf Anwendungsebene mit einem Protokoll wie Transport Layer Security (TLS) verwenden. Weitere Informationen zur Verschlüsselung des EC2-Instance-Datenverkehrs finden Sie unter Verschlüsselung bei der Übertragung im Amazon EC2-Benutzerhandbuch.

> **Note**
>
> Die Nitro-Netzwerkverschlüsselung gilt nicht für die EC2-Instances, die Amazon EVS bereitstellt. Amazon EVS unterstützt keine Verschlüsselung während der Übertragung von Datenverkehr zwischen Hosts.

Verschlüsselungsoptionen während der Übertragung für lokale Konnektivität

Um den Verkehr zwischen Ihrem lokalen Rechenzentrum und Amazon EVS zu verschlüsseln, können Sie AWS Direct Connect und AWS Site-To-Site VPN mit AWS Transit Gateway kombinieren. Diese Kombination bietet eine IPsec verschlüsselte private Verbindung, die auch die Netzwerkkosten senkt, den Bandbreitendurchsatz erhöht und ein konsistenteres Netzwerkerlebnis bietet als internetbasierte VPN-Verbindungen. Weitere Informationen finden Sie unter Privates AWS Site-to-Site IP-VPN mit AWS Direct Connect.

> **Note**
>
> Amazon EVS unterstützt keine Konnektivität über eine private virtuelle Schnittstelle (VIF) von AWS Direct Connect oder über eine AWS Site-to-Site VPN-Verbindung, die direkt mit der Underlay-VPC endet. Amazon EVS unterstützt IPSec VPN-Terminierung auf dem NSX Edge

Tier-0- oder Tier-1-Gateway. Weitere Informationen finden Sie unter Hinzufügen eines NSX-VPN-Dienstes in der NSX-Dokumentation IPSec . VMware

MAC Security (MACsec) ist ein IEEE-Standard, der Datenvertraulichkeit, Datenintegrität und Authentizität der Datenherkunft gewährleistet. Sie können AWS Direct Connect-Verbindungen verwenden, die MACsec die Verschlüsselung Ihrer Daten von Ihrem Unternehmensrechenzentrum zum AWS Direct Connect-Standort unterstützen. Weitere Informationen finden Sie unter MAC-Sicherheit in AWS Direct Connect im AWS Direct Connect-Benutzerhandbuch.

Verschlüsselung bei der Übertragung von VMware Netzwerkdaten

Nach der Bereitstellung der Amazon EVS-Umgebung haben Sie mehrere Optionen, um die Verschlüsselung von Daten bei der Übertragung auf der VMware VCF-Ebene durchzusetzen:

- VMware vDefend Distributed Firewall — Ermöglicht die Implementierung einer detaillierten Netzwerksegmentierung und die Durchsetzung der Verschlüsselung zwischen virtuellen Maschinen. TLS/SSL Weitere Informationen finden Sie in der VCF-Dokumentation unter Konfigurieren der Sicherheitseinstellungen für die verteilte Firewall mithilfe der Benutzeroberfläche. VMware
- data-in-transitvSAN-Verschlüsselung — Kann verwendet werden, um alle Daten und Metadaten zwischen Hosts in Ihrem vSAN-Cluster zu verschlüsseln. Weitere Informationen finden Sie unter Data-In-TransitvSAN-Verschlüsselung in der VMware vSAN-Dokumentation.
- Verschlüsseltes vSphere vMotion — gewährleistet Vertraulichkeit, Integrität und Authentizität von Daten, die mit vSphere vMotion übertragen werden. Weitere Informationen finden Sie unter Was ist verschlüsseltes vSphere vMotion in der vSphere-Dokumentation.

Verwaltung von Schlüsseln und Geheimnissen

Während der Bereitstellung der Amazon EVS-Umgebung verwendet Amazon EVS AWS Secrets Manager, um Secrets zu erstellen, zu verschlüsseln und zu speichern, die die VCF-Anmeldeinformationen enthalten, die für die Installation und den Zugriff auf VMware VCF-Verwaltungs-Appliances sowie das ESX-Root-Passwort erforderlich sind. Amazon EVS löscht auch verwaltete Geheimnisse in Ihrem Namen, wenn die EVS-Umgebung gelöscht wird. Weitere Informationen finden Sie unter Was ist in einem Secrets Manager Manager-Geheimnis im AWS Secrets Manager-Benutzerhandbuch.

Secrets Manager verwendet eine Umschlagverschlüsselung mit AWS KMS Schlüsseln und Datenschlüsseln, um jeden geheimen Wert zu schützen. Sofern nicht anders angegeben, wird der AWS verwaltete Standardschlüssel für Secrets Manager verwendet. Alternativ können Sie bei der Erstellung der Umgebung einen vom Kunden verwalteten Schlüssel angeben, um Ihre Geheimnisse zu verschlüsseln. Weitere Informationen finden Sie unter Secrets Ver- und Entschlüsselung in AWS Secrets Manager im AWS Secrets Manager Manager-Benutzerhandbuch.

> **Note**
>
> Für vom Kunden verwaltete Schlüssel fallen zusätzliche Nutzungsgebühren an. Der AWS verwaltete Standardschlüssel wird kostenlos zur Verfügung gestellt. Weitere Informationen finden Sie unter Preise im AWS Secrets Manager Manager-Benutzerhandbuch.

Amazon EVS synchronisiert nach der Bereitstellung keine Anmeldeinformationen zwischen AWS Secrets Manager und Ihrer VCF-Software. Sie sind dafür verantwortlich, dass die mit Ihrer Amazon EVS-Umgebung verknüpften Geheimnisse mit den Anmeldeinformationen im SDDC Manager synchronisiert werden, um den Ablauf von VCF-Passwörtern und den Verlust des Zugriffs auf die VCF-Software zu verhindern.

Amazon EVS wechselt Geheimnisse nicht in Ihrem Namen. Sie sind dafür verantwortlich, die mit Ihrer Umgebung verknüpften Geheimnisse rotieren zu lassen. Wir empfehlen dringend, Ihre Geheimnisse rotieren zu lassen, sobald die Umgebung erstellt wurde, und einen Rotationsplan zu implementieren, um Ihre Geheimnisse in regelmäßigen Abständen zu aktualisieren. Weitere Informationen zur Rotation von AWS Secrets Manager Manager-Geheimnissen finden Sie unter Rotation durch Lambda-Funktion im AWS Secrets Manager Manager-Benutzerhandbuch. Weitere Informationen zur VCF-Passwortverwaltung finden Sie unter Passwortverwaltung in der VMware Cloud Foundation-Dokumentation.

> **Important**
>
> Amazon EVS synchronisiert nach der Bereitstellung keine Anmeldeinformationen zwischen AWS Secrets Manager und Ihrer VCF-Software. Wenn Sie AWS Secrets Manager nach der Bereitstellung verwenden, müssen Sie die Anmeldeinformationen zwischen AWS Secrets Manager und SDDC Manager synchron halten, um Probleme mit dem Ablauf von VCF-Passwörtern zu vermeiden. Sie verlieren möglicherweise den Zugriff auf die VCF-Software,

wenn die SDDC Manager-Anmeldeinformationen nicht auf dem neuesten Stand gehalten werden.

> **Note**
>
> Amazon EVS bietet keine verwaltete Rotation von Geheimnissen.

> **Note**
>
> Die Verwendung einer Lambda-Funktion für die geheime Rotation von AWS Secrets Manager ist mit Kosten verbunden. Weitere Informationen finden Sie unter Preise im AWS Secrets Manager Manager-Benutzerhandbuch.

Richtlinie für den Datenverkehr zwischen Netzwerken

Amazon EVS verwendet eine vom Kunden bereitgestellte VPC, um Grenzen zwischen Ressourcen in der Amazon EVS-Umgebung zu schaffen und den Verkehr zwischen ihnen, Ihrem lokalen Netzwerk und dem Internet zu kontrollieren. Weitere Informationen zur Amazon VPC Sicherheit finden Sie im Benutzerhandbuch unter Gewährleisten des Datenschutzes im Netzwerkverkehr. Amazon VPC Amazon VPC

Standardmäßig erstellt Amazon EVS während der Umgebungserstellung private VLAN-Subnetze, die den direkten Internetzugang verweigern. Um Ihrer VPC eine weitere Sicherheitsebene hinzuzufügen, können Sie eine benutzerdefinierte Netzwerkzugriffskontrollliste für Ihre VPC mit Regeln erstellen, die die Internetkonnektivität weiter einschränken. Weitere Informationen finden Sie unter Erstellen einer Netzwerk-ACL für Ihre VPC im Amazon VPC-Benutzerhandbuch.

> **Important**
>
> EC2-Sicherheitsgruppen funktionieren nicht auf elastischen Netzwerkschnittstellen, die mit Amazon EVS-VLAN-Subnetzen verbunden sind. Um den Verkehr zu und von Amazon EVS VLAN-Subnetzen zu kontrollieren, müssen Sie eine Netzwerkzugriffskontrollliste verwenden.

Wenn Sie ein NSX-Administrator sind, können Sie die folgenden NSX-Funktionen zur Sicherung des Netzwerkverkehrs konfigurieren:

- VMware vDefend Gateway Firewall — Schützt den Netzwerkperimeter und schützt vor externen Bedrohungen (Nord-Süd-Verkehr). Weitere Informationen finden Sie unter Hinzufügen einer Gateway-Firewall-Richtlinie und -Regel in der NSX-Dokumentation. VMware
- VMware vDefend Distributed Firewall — Schützt vor Angriffen aus einem internen Netzwerk (Ost-West-Verkehr). Weitere Informationen finden Sie unter Hinzufügen einer verteilten Firewall in der VMware NSX-Dokumentation.

Identitäts- und Zugriffsmanagement für Amazon Elastic VMware Service

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf AWS Ressourcen sicher zu kontrollieren. IAM Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Amazon Elastic VMware Service (Amazon EVS) -Ressourcen zu nutzen. IAM ist eine AWS-Service , die Sie ohne zusätzliche Kosten nutzen können.

Themen

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt davon ab, welche Arbeit Sie in Amazon EVS ausführen.

Servicebenutzer — Wenn Sie den Amazon EVS-Service für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen zur Verfügung, die Sie benötigen. Da Sie für Ihre Arbeit mehr Amazon EVS-Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anfordern müssen.

Wenn Sie auf eine Funktion in Amazon EVS nicht zugreifen können, finden Sie weitere Informationen unterthe section called “Fehlerbehebung bei Amazon EVS-Identität und -Zugriff”.

Service-Administrator — Wenn Sie in Ihrem Unternehmen für die Amazon EVS-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf Amazon EVS. Es ist Ihre Aufgabe, zu bestimmen, auf welche Amazon EVS-Funktionen und -Ressourcen Ihre Servicebenutzer zugreifen sollen. Anschließend müssen Sie Anfragen an Ihren IAM Administrator senden, um die Berechtigungen Ihrer Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die grundlegenden Konzepte von zu verstehen IAM. Weitere Informationen darüber, wie Ihr Unternehmen Amazon EVS nutzen IAM kann, finden Sie unterthe section called “So funktioniert Amazon EVS mit IAM”.

IAM Administrator — Wenn Sie ein IAM Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff auf Amazon EVS zu verwalten. Beispiele für identitätsbasierte Amazon EVS-Richtlinien, die Sie in IAM verwenden können, finden Sie unter. the section called “Beispiele für identitätsbasierte Amazon EVS-Richtlinien”

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als Root-Benutzer des AWS Kontos authentifiziert (angemeldet AWS) sein IAM-Benutzer, oder indem Sie eine IAM Rolle übernehmen.

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) Nutzer, die Single-Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als föderierte Identität anmelden, hat Ihr Administrator zuvor einen Identitätsverbund mithilfe von Rollen eingerichtet. IAM Wenn Sie AWS mithilfe eines Verbunds darauf zugreifen, übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS-Managementkonsole oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie unter So melden Sie sich bei Ihrem an AWS-Konto im AWS Anmelde-Benutzerhandbuch. AWS

Wenn Sie AWS programmgesteuert zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, um Ihre Anfragen mit Ihren Anmeldeinformationen kryptografisch zu signieren. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu signieren, finden Sie unter Signaturvorgang für Signature Version 4 in der AWS Allgemeinen Referenz.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise auch zusätzliche Sicherheitsinformationen angeben. AWS Empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Multi-Factor Authentication im AWS IAM Identity Center (Nachfolger von AWS Single Sign-On) User Guide und Using Multi-Factor Authentication (MFA) AWS im IAM-Benutzerhandbuch.

AWS Konto (Root-Benutzer)

Wenn Sie zum ersten Mal einen erstellen AWS-Konto, beginnen Sie mit einer einzigen Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als Root-Benutzer des AWS Kontos bezeichnet. Der Zugriff erfolgt, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für alltägliche Aufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie im Referenzhandbuch zur Kontoverwaltung unter Aufgaben, für die Root-Benutzeranmeldedaten erforderlich sind.

Verbundidentität

Es hat sich bewährt, menschlichen Benutzern, einschließlich Benutzern, die Administratorzugriff benötigen, vorzuschreiben, den Verbund mit einem Identitätsanbieter zu verwenden, um AWS-Services mithilfe temporärer Anmeldeinformationen darauf zugreifen zu können.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center (Nachfolger von AWS Single Sign-On) -Benutzerhandbuch.

IAM-Benutzer und Gruppen

Eine IAM-Benutzerist eine Identität innerhalb von Ihnen AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wir empfehlen, sich nach Möglichkeit auf temporäre Zugangsdaten zu verlassen IAM-Benutzer , anstatt solche mit langfristigen Zugangsdaten wie Passwörtern und Zugangsschlüsseln zu erstellen. Wenn Sie jedoch spezielle Anwendungsfälle haben, für die langfristige Anmeldeinformationen erforderlich sind, empfehlen wir IAM-Benutzer, dass Sie die Zugriffsschlüssel rotieren. Weitere Informationen finden Sie unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Eine IAM Gruppe ist eine Identität, die eine Sammlung von angibt IAM-Benutzer. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen erleichtern die Verwaltung von Berechtigungen für große Benutzergruppen. Sie könnten beispielsweise einer Gruppe einen Namen geben IAMAdminsund dieser Gruppe Berechtigungen zur Verwaltung von IAM Ressourcen erteilen.

Benutzer sind nicht dasselbe wie Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Wann sollte eine Rolle IAM-Benutzer (statt einer Rolle) erstellt werden?

IAM Rollen

Eine IAM Rolle ist eine Identität innerhalb von Ihnen AWS-Konto , für die bestimmte Berechtigungen gelten. Sie ähnelt einer IAM-Benutzer, ist aber keiner bestimmten Person zugeordnet. Sie können vorübergehend eine IAM Rolle in der übernehmen, AWS-Managementkonsole indem Sie die Rollen wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden zur Verwendung von Rollen finden Sie unter IAM Rollen verwenden im IAM-Benutzerhandbuch.

IAM Rollen mit temporären Anmeldeinformationen sind in den folgenden Situationen nützlich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Um zu steuern, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center (Nachfolger von AWS Single Sign-On) -Benutzerhandbuch.
- Temporäre IAM-Benutzer Berechtigungen — Ein Benutzer IAM-Benutzer kann eine IAM Rolle übernehmen, um vorübergehend verschiedene Berechtigungen für eine bestimmte Aufgabe zu übernehmen.
- Kontoübergreifender Zugriff — Sie können eine IAM Rolle verwenden, um jemandem (einem vertrauenswürdigen Principal) in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zum Unterschied zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie im IAM-Benutzerhandbuch unter Unterschiede zwischen IAM Rollen und ressourcenbasierten Richtlinien.
- Serviceübergreifender Zugriff — Einige verwenden Funktionen in anderen. AWS-Services AWS-Services Wenn Sie beispielsweise in einem Dienst einen Anruf tätigen, ist es üblich, dass dieser Dienst Anwendungen ausführt Amazon EC2 oder Objekte darin Amazon S3 speichert. Ein Service kann dies mithilfe der Berechtigungen des aufrufenden Prinzipals, einer Servicerolle oder einer serviceverknüpften Rolle tun.
  - Hauptberechtigungen — Wenn Sie eine IAM-Benutzer OR-Rolle verwenden, um Aktionen in auszuführen AWS, gelten Sie als Principal. Richtlinien erteilen einem Prinzipal-Berechtigungen. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen.
  - Servicerolle — Eine Servicerolle ist eine IAM Rolle, die ein Dienst übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM Administrator kann eine Servicerolle von innen heraus erstellen, ändern und löschen IAM. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

  - Dienstbezogene Rolle — Eine dienstverknüpfte Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM Administrator kann die Berechtigungen für dienstbezogene Rollen anzeigen, aber nicht bearbeiten.
- Anwendungen, die auf einer Instanz ausgeführt werden Amazon EC2 — Sie können eine IAM Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer Amazon EC2 Instanz ausgeführt werden und AWS API-Anfragen stellen AWS CLI . Dies ist dem Speichern von Zugriffsschlüsseln innerhalb der Amazon EC2 Instanz vorzuziehen. Um einer Amazon EC2 Instanz eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instanzprofil, das an die Instanz angehängt ist. Ein Instanzprofil enthält die Rolle und ermöglicht Programmen, die auf der Amazon EC2 Instanz ausgeführt werden, temporäre Anmeldeinformationen abzurufen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Verwenden einer IAM Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon EC2 Instances ausgeführt werden.

Informationen zur Verwendung von IAM Rollen finden Sie im IAM-Benutzerhandbuch unter Wann IAM sollte eine Rolle (anstelle eines Benutzers) erstellt werden?.

Verwalten des Zugriffs mit Richtlinien

Sie steuern den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Die Berechtigungen in den Richtlinien legen fest, ob eine Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Jede IAM Entität (Benutzer oder Rolle) beginnt ohne Berechtigungen. Standardmäßig können Benutzer nichts tun, nicht einmal ihr eigenes Passwort ändern. Um einem Benutzer die Berechtigung für eine Aktion zu erteilen, muss ein Administrator einem Benutzer eine Berechtigungsrichtlinie

zuweisen. Alternativ kann der Administrator den Benutzer zu einer Gruppe hinzufügen, die über die gewünschten Berechtigungen verfügt. Wenn ein Administrator einer Gruppe Berechtigungen erteilt, erhalten alle Benutzer in dieser Gruppe diese Berechtigungen.

IAM Richtlinien definieren Berechtigungen für eine Aktion, unabhängig von der Methode, mit der Sie den Vorgang ausführen. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der AWS-Managementkonsole AWS CLI, der oder der AWS API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind Richtliniendokumente für JSON-Berechtigungen, die Sie an eine Identität, z. B. eine Rolle oder Gruppe IAM-Benutzer, anhängen können. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen einer identitätsbasierten Richtlinie finden Sie unter Erstellen von IAM Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Eingebundene Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können. AWS-Konto Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter Auswahl zwischen verwalteten und eingebundenen Richtlinien im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource wie einen Amazon S3 Bucket anhängen. Serviceadministratoren können mit diesen Richtlinien festlegen, welche Aktionen ein angegebener Prinzipal (Kontomitglied, Benutzer oder Rolle) für diese Ressource durchführen kann, und unter welchen Bedingungen dies möglich ist. Ressourcenbasierte Richtlinien sind Inline-Richtlinien. Es gibt keine verwalteten ressourcenbasierten Richtlinien.

Zugriffskontrolllisten () ACLs

Zugriffskontrolllisten (ACLs) sind eine Art von Richtlinie, mit der gesteuert wird, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-

Richtliniendokumentformat. Amazon S3 AWS WAF, und Amazon VPC sind Beispiele für Dienste, die Unterstützung bieten. ACLs Weitere Informationen finden Sie in der Übersicht über ACLs die Access Control List (ACL) im Amazon Simple Storage Service Developer Guide.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Mit diesen Richtlinientypen können Sie die maximalen Berechtigungen festlegen, die Ihnen durch die gängigeren Richtlinientypen gewährt werden.

- Berechtigungsgrenzen — Eine Berechtigungsgrenze ist eine erweiterte Funktion, mit der Sie die maximalen Berechtigungen festlegen, die eine identitätsbasierte Richtlinie einer IAM Entität (IAM-Benutzer oder Rolle) gewähren kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die resultierenden Berechtigungen sind die Schnittmenge der identitätsbasierten Richtlinien der Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen zu Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM Entitäten im IAM-Benutzerhandbuch.
- Dienststeuerungsrichtlinien (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in AWS Organizations festlegen. AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie alle Funktionen in einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen AWS Root-Benutzer. Weitere Informationen zu Organizations und SCPs finden Sie unter How SCPs Work im AWS Organizations User Guide.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind die Schnittmenge der identitätsbasierten Richtlinien des Benutzers oder der Rolle und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn für eine Anfrage mehrere Arten von Richtlinien gelten, sind die sich daraus ergebenden Berechtigungen schwieriger zu verstehen. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie unter Bewertungslogik für Richtlinien im IAM-Benutzerhandbuch.

So funktioniert Amazon EVS mit IAM

Informieren Sie sich vor der Nutzung IAM zur Verwaltung des Zugriffs auf Amazon EVS darüber, welche IAM Funktionen für Amazon EVS verfügbar sind.

IAM Funktion	Amazon EVS-Unterstützung
the section called “Identitätsbasierte Richtlinien für Amazon EVS”	Ja
the section called “Ressourcenbasierte Richtlinien innerhalb von Amazon EVS”	Nein
the section called “Politische Maßnahmen für Amazon EVS”	Ja
the section called “Richtlinienressourcen für Amazon EVS”	Teilweise
the section called “Schlüssel für Richtlinienbedingungen für Amazon EVS”	Ja
the section called “Zugriffskontrolllisten (ACLs) in Amazon EVS”	Nein
the section called “Attributbasierte Zugriffskontrolle (ABAC) mit Amazon EVS”	Ja
the section called “Temporäre Anmeldeinformationen mit Amazon EVS verwenden”	Ja
the section called “Zugriffssitzungen für Amazon EVS weiterleiten”	Ja

IAM Funktion	Amazon EVS-Unterstützung
the section called “Servicerollen für Amazon EVS”	Nein
the section called “Servicebezogene Rollen für Amazon EVS”	Ja

Einen umfassenden Überblick darüber, wie Amazon EVS und andere AWS-Services Unternehmen AWS-Services damit arbeiten IAM, finden Sie IAM im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien für Amazon EVS

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Mit IAM identitätsbasierten Richtlinien können Sie zulässige oder verweigerte Aktionen und Ressourcen sowie die Bedingungen angeben, unter denen Aktionen zugelassen oder verweigert werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, der er zugeordnet ist. Weitere Informationen zu allen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie im IAM-Benutzerhandbuch unter Referenz zu IAM JSON-Richtlinienelementen.

Beispiele für identitätsbasierte Richtlinien für Amazon EVS

Beispiele für identitätsbasierte Amazon EVS-Richtlinien finden Sie unter. the section called “Beispiele für identitätsbasierte Amazon EVS-Richtlinien”

Ressourcenbasierte Richtlinien innerhalb von Amazon EVS

Unterstützt ressourcenbasierte Richtlinien: Nein

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und

Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource unterscheiden AWS-Konten, muss ein IAM-Administrator des vertrauenswürdigen Kontos auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie unter Kontenübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Politische Maßnahmen für Amazon EVS

Unterstützt Aktionen Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das `Action` Element einer IAM identitätsbasierten Richtlinie beschreibt die spezifischen Aktionen, die durch die Richtlinie zugelassen oder verweigert werden. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Die Aktion wird in einer Richtlinie verwendet, um Berechtigungen zur Durchführung der zugehörigen Aktion zu gewähren.

Richtlinienaktionen in Amazon EVS verwenden das folgende Präfix vor der Aktion:`evs:`.
Um beispielsweise jemandem die Erlaubnis zu erteilen, eine Umgebung mit dem Amazon `CreateEnvironment` EVS-API-Vorgang zu erstellen, nehmen Sie die `evs:CreateEnvironment` Aktion in seine Richtlinie auf. Richtlinienanweisungen müssen entweder ein – `Action`oder ein `NotAction`-Element enthalten. Amazon EVS definiert eigene Aktionen, die Aufgaben beschreiben, die Sie mit diesem Service ausführen können.

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie wie folgt durch Kommata:

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

Sie können auch Platzhalter verwenden, um mehrere Aktionen anzugeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `List` beginnen, einschließlich der folgenden Aktion:

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

Eine Liste der Amazon EVS-Aktionen finden Sie unter Von Amazon EVS definierte Aktionen in der Service Authorization Reference.

Richtlinienressourcen für Amazon EVS

Unterstützt Richtlinienressourcen: teilweise

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

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

Eine Liste der Amazon EVS-Ressourcentypen und ihrer ARNs Eigenschaften finden Sie unter Von Amazon Elastic VMware Service definierte Ressourcen in der Service Authorization Reference. Informationen darüber, mit welchen Aktionen Sie den ARN jeder Ressource angeben können, finden Sie unter Von Amazon Elastic VMware Service definierte Aktionen.

Einige Amazon EVS-API-Aktionen unterstützen mehrere Ressourcen. Beispielsweise können beim Aufrufen der `ListEnvironments` API-Aktion mehrere Umgebungen referenziert werden. Um mehrere Ressourcen in einer einzigen Anweisung anzugeben, trennen Sie sie ARNs durch Kommas.

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

Die Amazon EVS-Umgebungsressource hat beispielsweise den folgenden ARN:

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

Verwenden Sie das folgende Beispiel ARNs, um die Umgebungen `my-environment-1` und `my-environment-2` in Ihrem Statement zu spezifizieren:

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

Um alle Umgebungen anzugeben, die zu einem bestimmten Konto gehören, verwenden Sie den Platzhalter (*):

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

Schlüssel für Richtlinienbedingungen für Amazon EVS

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Mit dem `Condition` Element (oder `Condition` Block) können Sie die Bedingungen angeben, unter denen eine Aussage gültig ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen `AND`-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen `OR` Operation aus. Alle Bedingungen müssen erfüllt sein, bevor die Berechtigungen für die Anweisung erteilt werden.

Sie können bei der Angabe von Bedingungen auch Platzhaltervariablen verwenden. Sie können beispielsweise nur dann eine IAM-Benutzer Zugriffsberechtigung für eine Ressource erteilen, wenn sie mit ihrem IAM-Benutzer Namen gekennzeichnet ist. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter IAM Richtlinienelemente: Variablen und Tags.

Amazon EVS definiert seinen eigenen Satz von Bedingungsschlüsseln und unterstützt auch die Verwendung einiger globaler Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontext-Schlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Alle Amazon EC2 Aktionen unterstützen die `ec2:Region` Bedingungstasten `aws:RequestedRegion` und. Weitere Informationen finden Sie unter Beispiel: Beschränken des Zugriffs auf eine bestimmte Region.

Eine Liste der Amazon EVS-Bedingungsschlüssel finden Sie unter Condition Keys for Amazon EVS in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von Amazon EVS definierte Aktionen.

Zugriffskontrolllisten (ACLs) in Amazon EVS

Unterstützt ACLs: Nein

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Attributbasierte Zugriffskontrolle (ABAC) mit Amazon EVS

Unterstützt ABAC (Tags in Richtlinien): Ja

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In werden diese AWS Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag auf der Ressource übereinstimmt, auf die er zugreifen möchte.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Sie können Tags an Amazon EVS-Ressourcen anhängen oder Tags in einer Anfrage an Amazon EVS übergeben. Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/<key-name>`, `aws:RequestTag/<key-name>`, oder Bedingung `aws:TagKeys` verwenden. Weitere Informationen darüber, mit welchen Aktionen Sie Tags in Bedingungsschlüsseln verwenden können, finden Sie unter Von Amazon EVS definierte Aktionen in der Service Authorization Reference.

Temporäre Anmeldeinformationen mit Amazon EVS verwenden

Unterstützt temporäre Anmeldeinformationen: Ja

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären Anmeldeinformationen AWS-Services funktionieren AWS-Services , finden Sie im IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS-Managementkonsole Methode als einem Benutzernamen und einem Passwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter Wechseln von einer Benutzerrolle zu einer IAM-Rolle (Konsole) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Zugriffssitzungen für Amazon EVS weiterleiten

Unterstützt Forward Access Sessions (FAS): Ja

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren

Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anforderungen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für Amazon EVS

Unterstützt Servicerollen: Nein

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

Servicebezogene Rollen für Amazon EVS

Unterstützt serviceverknüpfte Rollen: Ja

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Einzelheiten zum Erstellen oder Verwalten von serviceverknüpften Amazon EVS-Rollen finden Sie unter. the section called “Verwenden von servicegebundenen Rollen”

Beispiele für identitätsbasierte Amazon EVS-Richtlinien

Standardmäßig sind Rollen nicht berechtigt, IAM-Benutzer Amazon EVS-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mit der AWS-Managementkonsole AWS CLI, oder AWS API ausführen. Ein IAM Administrator muss IAM Richtlinien erstellen, die Benutzern und Rollen die Erlaubnis gewähren, bestimmte API-Operationen mit den angegebenen Ressourcen auszuführen, die sie benötigen. Der Administrator muss diese Richtlinien dann den Gruppen IAM-Benutzer oder Gruppen zuordnen, für die diese Berechtigungen erforderlich sind.

Informationen zum Erstellen einer identitätsbasierten IAM-Richtlinie mithilfe dieser Beispieldokumente zu JSON-Richtlinien finden Sie unter Erstellen von Richtlinien mit dem JSON-Editor im IAM-Benutzerhandbuch.

Themen

- Best Practices für Richtlinien

- Verwenden der Amazon EVS-Konsole
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer
- Erstellen und verwalten Sie eine Amazon EVS-Umgebung
- Abrufen und Auflisten von Amazon EVS-Umgebungen, Hosts und VLANs

Best Practices für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand Amazon EVS-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder diese löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Wenn Sie identitätsbasierte Richtlinien erstellen oder bearbeiten, befolgen Sie diese Richtlinien und Empfehlungen:

- Erste Schritte mit AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um damit zu beginnen, Ihren Benutzern und Workloads Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien oder Von AWS verwaltete Richtlinien für Auftragsfunktionen im IAM-Benutzerhandbuch.
- Berechtigungen mit den geringsten Rechten anwenden — Wenn Sie Berechtigungen mit IAM Richtlinien festlegen, gewähren Sie nur die Berechtigungen, die für die Ausführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen IAM im IAM-Benutzerhandbuch.
- Verwenden Sie Bedingungen in IAM Richtlinien, um den Zugriff weiter einzuschränken — Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen einzuschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese im Rahmen einer bestimmten Aktion verwendet werden AWS-Service, z. CloudFormation B. Weitere Informationen finden Sie unter IAM JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Wird verwendet IAM Access Analyzer , um Ihre IAM Richtlinien zu validieren, um sichere und funktionale Berechtigungen zu gewährleisten — IAM Access Analyzer validiert neue und

bestehende Richtlinien, sodass die Richtlinien der IAM Richtliniensprache (JSON) und den IAM Best Practices entsprechen. IAM Access Analyzer bietet mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen, um Sie bei der Erstellung sicherer und funktionaler Richtlinien zu unterstützen. Weitere Informationen finden Sie unter IAM Access Analyzer Richtlinienvalidierung im IAM-Benutzerhandbuch.

- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das Root-Benutzer in Ihrem Konto erfordert IAM-Benutzer , aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Konfigurieren eines MFA-geschützten API-Zugriffs im IAM-Benutzerhandbuch.

Verwenden der Amazon EVS-Konsole

Um auf die Amazon EVS-Konsole zugreifen zu können, muss ein IAM-Principal über Mindestberechtigungen verfügen. Diese Berechtigungen müssen es dem Principal ermöglichen, Details zu den Amazon EVS-Ressourcen in Ihrem AWS-Konto aufzulisten und anzuzeigen. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die restriktiver als die mindestens erforderlichen Berechtigungen ist, funktioniert die Konsole für Prinzipals, denen diese Richtlinie zugewiesen ist, nicht wie vorgesehen.

Um sicherzustellen, dass Ihre IAM-Prinzipale die Amazon EVS-Konsole weiterhin verwenden können, erstellen Sie eine Richtlinie mit Ihrem eigenen eindeutigen Namen, z. B. `AmazonEVSAdminPolicy` Hängen Sie die Richtlinie an die Prinzipale an. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer imIAM-Benutzerhandbuch:

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

Sie müssen Benutzern, die nur die API AWS CLI oder die API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. AWS Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die Sie ausführen möchten.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Dieses Beispiel zeigt, wie Sie eine Richtlinie erstellen könnten, die es IAM-Benutzer ermöglicht, die internen und verwalteten Richtlinien anzuzeigen, die mit ihrer Benutzeridentität verknüpft sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der API AWS CLI oder 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": "*"
        }
    ]
}
```

Erstellen und verwalten Sie eine Amazon EVS-Umgebung

Diese Beispielrichtlinie umfasst die Berechtigungen, die erforderlich sind, um eine Amazon EVS-Umgebung zu erstellen und zu löschen und Hosts hinzuzufügen oder zu löschen, nachdem die Umgebung erstellt wurde.

Sie können die durch die AWS-Region ersetzen AWS-Region , in der Sie eine Umgebung erstellen möchten. Wenn Ihr Konto bereits über die `AWSServiceRoleForAmazonEVS`-Rolle verfügt, können Sie die `iam:CreateServiceLinkedRole`-Aktion aus der Richtlinie entfernen. Wenn Sie jemals eine Amazon EVS-Umgebung in Ihrem Konto erstellt haben, ist eine Rolle mit diesen Berechtigungen bereits vorhanden, sofern Sie sie nicht gelöscht haben.

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

Abrufen und Auflisten von Amazon EVS-Umgebungen, Hosts und VLANs

Diese Beispielrichtlinie umfasst die Mindestberechtigungen, die ein Administrator zum Abrufen und Auflisten aller Amazon EVS-Umgebungen, Hosts und VLANs innerhalb eines bestimmten Kontos in den AWS-Region us-east-2.

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

Fehlerbehebung bei Amazon EVS-Identität und -Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit Amazon EVS und IAM auftreten können.

Themen

- AccessDeniedException
- Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Amazon EVS-Ressourcen ermöglichen

AccessDeniedException

Wenn Sie `AccessDeniedException` beim Aufrufen einer AWS API-Operation eine Meldung erhalten, verfügen die von Ihnen verwendeten IAM-Prinzipalanmeldedaten nicht über die erforderlichen Berechtigungen, um diesen Aufruf durchzuführen.

```
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
```

In der vorherigen Beispielnachricht hat der Benutzer keine Berechtigungen, den Amazon `CreateEnvironment` EVS-API-Vorgang aufzurufen. Informationen zum Erteilen von Amazon EVS-Administratorberechtigungen für einen IAM-Prinzipal finden Sie unter. the section called “Beispiele für identitätsbasierte Amazon EVS-Richtlinien”

Weitere allgemeine Informationen zu IAM finden Sie unter Steuern des Zugriffs auf AWS Ressourcen mithilfe von Richtlinien im IAM-Benutzerhandbuch.

Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Amazon EVS-Ressourcen ermöglichen

Sie können eine Rolle erstellen, mit der Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation auf Ihre Ressourcen zugreifen können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob Amazon EVS diese Funktionen unterstützt, finden Sie unterthe section called “So funktioniert Amazon EVS mit IAM”.
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie IAM-Benutzer im IAM-Benutzerhandbuch unter Gewähren des Zugriffs auf eine andere Ressource AWS-Konto , die Ihnen gehört.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs auf Ressourcen, die AWS-Konten Eigentum Dritter sind.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie im IAM-Benutzerhandbuch unter Unterschiede zwischen IAM Rollen und ressourcenbasierten Richtlinien.

AWS verwaltete Richtlinien für Amazon EVS

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet AWS wird. AWS Verwaltete Richtlinien dienen dazu, Berechtigungen für viele gängige Anwendungsfälle bereitzustellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie allen AWS Kunden zur Verfügung stehen. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden. Weitere Informationen finden Sie im IAM Benutzerhandbuch unter AWS Verwaltete Richtlinien.

AWS verwaltete Richtlinie: Amazon EVSService RolePolicy

Sie können `AmazonEVSServiceRolePolicy` nicht an Ihre IAM-Entitäten anfügen. Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es Amazon EVS ermöglicht, Aktionen in Ihrem Namen durchzuführen. Weitere Informationen finden Sie unter the section called “Verwenden von servicegebundenen Rollen”. Wenn Sie eine Umgebung mit einem IAM-Prinzipal erstellen, der über die `iam:CreateServiceLinkedRole` entsprechende Berechtigung verfügt, wird die `AWSServiceRoleforAmazonEVS` serviceverknüpfte Rolle automatisch für Sie erstellt, wobei diese Richtlinie an sie angehängt ist.

Diese Richtlinie ermöglicht es der `AWSServiceRoleForAmazonEVS` serviceverknüpften Rolle, in Ihrem Namen Anrufe AWS-Services zu tätigen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen, die es Amazon EVS ermöglichen, die folgenden Aufgaben auszuführen.

- `ec2`- Entdecken Sie VPC-Netzwerkkomponenten, einschließlich Subnetze und. VPCs Erstellen, ändern, kennzeichnen und löschen Sie elastische Netzwerkschnittstellen, die zum Herstellen

einer dauerhaften Verbindung zwischen Amazon EVS und der VMware Virtual Cloud Foundation (VCF) SDDC Manager-Appliance in Ihrem VPC-Subnetz verwendet werden. Diese Konnektivität ist erforderlich, damit Amazon EVS die VCF-Bereitstellung bereitstellen, verwalten und überwachen kann.

- `ec2`- Löschen Sie EC2-Instances, die Amazon EVS erstellt, wenn Sie eine Anfrage zum Löschen eines EVS-Hosts stellen. Beschreiben und ändern Sie die EC2-Instance-Attribute, sodass der standardmäßige Schutz vor Kündigung und Stopp von EC2-Instances bei Bedarf deaktiviert werden kann, um das Löschen von EVS-Hosts zu unterstützen.
- `ec2`- Verwalten Sie EBS-Volumes für die Installation und Bereinigung von Cloud Builder. Während der Umgebungserstellung wird Cloud Builder auf einem der von Amazon EVS bereitgestellten Hosts installiert, um VCF-Konfigurationsänderungen vorzunehmen. Nach Abschluss entfernt Amazon EVS Cloud Builder, indem das EC2-Volume, auf dem es gespeichert ist, getrennt und gelöscht wird.
- `ec2`- Löschen Sie EVS-VLAN-Subnetze in Ihrem Namen, wenn Sie das Löschen der Umgebung beantragen.
- `secretsmanager`- Löschen Sie VCF-Passwörter, die Amazon EVS während der Umgebungserstellung im AWS Secrets Manager erstellt und speichert. Amazon EVS löscht alle Geheimnisse, die der Service in Ihrem Konto erstellt, wenn die Erstellung der Umgebung fehlschlägt oder wenn Sie das Löschen der Umgebung beantragen. Rufen Sie vCenter-Anmeldeinformationen von AWS Secrets Manager ab, wenn Sie einen vCenter-Connector konfigurieren, indem Sie einen geheimen ARN angeben. Die Berechtigung ist mit einer Ressourcen-Tag-Bedingung verknüpft, `EvsAccess=true` um sicherzustellen, dass Amazon EVS nur auf Geheimnisse zugreift, die explizit für den Zugriff auf Amazon EVS vCenter gekennzeichnet sind.
- `kms`- Entschlüsseln Sie Geheimnisse und beschreiben Sie KMS-Schlüssel, wenn die in Secrets Manager gespeicherten vCenter-Anmeldeinformationen mit KMS-Schlüsseln verschlüsselt werden. Die Berechtigung ist mit einer Ressourcen-Tag-Bedingung verknüpft, `EvsAccess=true` um sicherzustellen, dass Amazon EVS nur auf KMS-Schlüssel zugreift, die explizit für den vCenter-Zugriff gekennzeichnet sind.
- `cloudwatch`— Veröffentlichen Sie AWS Nutzungsmetriken CloudWatch für Amazon EVS-Ressourcen, für die Kontingente gelten.

Weitere Informationen zur Richtlinie, einschließlich der neuesten Version des JSON-Richtliniendokuments, finden Sie unter Amazon EVSService RolePolicy im AWS Managed Policy Reference Guide.

Amazon EVS-Updates für AWS verwaltete Richtlinien

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für Amazon EVS an, seit dieser Service begonnen hat, diese Änderungen zu verfolgen. Um automatische Warnungen über Änderungen an dieser Seite zu erhalten, abonnieren Sie den RSS-Feed auf der Dokumentverlauf-Seite.

Änderungen	Beschreibung	Date
Amazon EVSService RolePolicy — Richtlinie aktualisiert	Amazon EVS hat die Richtlinie aktualisiert, sodass der Service vCenter-Anmeldeinformationen von AWS Secrets Manager abrufen und mit KMS-Schlüsseln verschlüsselte Geheimnisse entschlüsseln kann. Weitere Informationen hierzu finden Sie unter the section called “AWS verwaltete Richtlinie: Amazon EVSService RolePolicy”.	23. März 2026
Amazon EVSService RolePolicy — Richtlinie aktualisiert	Amazon EVS hat die Richtlinie aktualisiert, um umfassende Ressourcenverwaltungsfunktionen wie EC2-Instance-Management, EBS-Volumenoperationen und AWS Secrets Manager Manager-Integration hinzuzufügen. Weitere Informationen hierzu finden Sie unter the section called “AWS verwaltete Richtlinie: Amazon EVSService RolePolicy”.	14. August 2025

Änderungen	Beschreibung	Date
Amazon EVSService RolePolicy — Richtlinie aktualisiert	Amazon EVS hat die Richtlinie aktualisiert, sodass der Service EVS-VLAN-Subnetze löschen und Amazon EVS-Nutzungsmetriken veröffentlichen kann. CloudWatch Weitere Informationen hierzu finden Sie unter the section called “AWS verwaltete Richtlinie: Amazon EVSService RolePolicy”.	14. Juli 2025
Amazon EVSService RolePolicy — Neue Richtlinie hinzugefügt	Amazon EVS hat eine neue Richtlinie hinzugefügt, die es dem Service ermöglicht, eine Verbindung zu einem VPC-Subnetz im Kundenkonto herzustellen. Diese Verbindung ist für die Servicefunktionalität erforderlich. Weitere Informationen hierzu finden Sie unter the section called “AWS verwaltete Richtlinie: Amazon EVSService RolePolicy”.	09. Juni 2025
Amazon EVS hat mit der Nachverfolgung von Änderungen begonnen	Amazon EVS hat damit begonnen, Änderungen an seinen AWS verwalteten Richtlinien nachzuverfolgen.	09. Juni 2025

Verwenden von serviceverknüpften Rollen für Amazon EVS

Amazon Elastic VMware Service verwendet serviceverknüpfte Rollen für AWS Identity and Access Management (IAM). Eine serviceverknüpfte Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit Amazon EVS verknüpft ist. Servicebezogene Rollen sind von Amazon EVS vordefiniert und beinhalten alle Berechtigungen, die der Service benötigt, um andere AWS Services in Ihrem Namen aufzurufen.

Eine serviceverknüpfte Rolle erleichtert die Einrichtung von Amazon EVS, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Amazon EVS definiert die Berechtigungen seiner serviceverknüpften Rollen, und sofern nicht anders definiert, kann nur Amazon EVS seine Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem ihre verwandten Ressourcen gelöscht wurden. Dadurch werden Ihre Amazon EVS-Ressourcen geschützt, da Sie die Zugriffsberechtigung für die Ressourcen nicht versehentlich entziehen können.

Informationen zu anderen Services, die serviceverknüpfte Rollen unterstützen, finden Sie unter AWS -Services, die mit IAM funktionieren. Suchen Sie nach den Services, für die Ja in der Spalte Serviceverknüpfte Rolle angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Servicebezogene Rollenberechtigungen für Amazon EVS

Amazon EVS verwendet die mit dem Service verknüpfte Rolle mit dem Namen. `AWSServiceRoleForAmazonEVS` Diese Rolle ermöglicht es Amazon EVS, Umgebungen in Ihrem Konto zu verwalten. Die beigefügte Richtlinie ermöglicht es der Rolle, die folgenden Ressourcen zu verwalten: elastische EVS-Netzwerkschnittstellen, EVS-VLAN-Subnetze, EVS-Hosts und Metriken. VPCs CloudWatch

Die serviceverknüpfte Rolle `AWSServiceRoleForAmazonEVS` vertraut darauf, dass die folgenden Services die Rolle annehmen:

- `evs.amazonaws.com`

Die Rollenberechtigungsrichtlinie ermöglicht es Amazon EVS, die folgenden Aktionen für die angegebenen Ressourcen durchzuführen:

- AmazonEVSServiceRolePolicy

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter Serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch.

Eine serviceverknüpfte Rolle für Amazon EVS erstellen

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie eine Umgebung in der AWS-Managementkonsole, der AWS CLI oder der AWS API erstellen, erstellt Amazon EVS die serviceverknüpfte Rolle für Sie.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie eine Umgebung erstellen, erstellt Amazon EVS die serviceverknüpfte Rolle erneut für Sie.

Bearbeiten einer serviceverknüpften Rolle für Amazon EVS

Amazon EVS erlaubt Ihnen nicht, die `AWSServiceRoleForAmazonEVS` serviceverknüpfte Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für Amazon EVS

Wenn Sie ein Feature oder einen Dienst, die bzw. der eine serviceverknüpften Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch Ihre serviceverknüpfte Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

Bereinigen einer serviceverknüpften Rolle

Bevor mit IAM eine serviceverknüpfte Rolle löschen können, müssen Sie zunächst alle von der Rolle verwendeten Ressourcen löschen. Schritte zum Löschen einer Amazon EVS-Umgebung mit Hosts finden Sie unterthe section called “Löschen Sie die Amazon EVS-Hosts und die Umgebung”.

> **Note**
>
> Wenn der Amazon EVS-Service die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Manuelles Löschen der -serviceverknüpften Rolle

Verwenden Sie die IAM-Konsole, die AWS CLI oder die AWS API, um die `AWSServiceRoleForAmazonEVS` serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Unterstützte Regionen für Amazon EVS-Rollen, die mit dem Service verknüpft sind

Amazon EVS unterstützt die Verwendung von serviceverknüpften Rollen in allen Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie unter Amazon Elastic VMware Service Endpoints and Quotas im AWS General Reference Guide.

Resilienz in Amazon EVS

Die AWS globale Infrastruktur basiert AWS-Regionen auf Availability Zones. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Amazon EVS-Umgebungen sind in einer einzigen AWS Availability Zone verfügbar. Um eine hohe Verfügbarkeit der Amazon EVS Single-AZ-Infrastruktur sicherzustellen, bietet Amazon EVS die folgenden Funktionen:

> **Note**
>
> Amazon EVS unterstützt derzeit nur Single-AZ-Bereitstellungen.

- Amazon EVS unterstützt die Verwendung von AWS Elastic Disaster Recovery zur Automatisierung der Sicherung und Wiederherstellung Ihrer Daten.
- Amazon EVS stellt einen Active/Standby NSX Edge-Cluster mit zwei NSX Edge-Knoten pro VCF-Anforderungen bereit. Die NSX Edge-Knoten werden auf verschiedenen Hosts ausgeführt, um eine hohe Verfügbarkeit zu gewährleisten und ein schnelles Failover für den seltenen Fall zu ermöglichen, dass ein NSX Edge-Knoten ausfällt.

- Amazon EVS stellt eine Minimalumgebung mit vier ESX-Hosts bereit, die für VCF erforderlich ist. Zusätzliche Hosts können nach der Bereitstellung hinzugefügt werden. Dies ist eine VMware Entwurfsanforderung, um ein ordnungsgemäßes vSAN-Quorum sicherzustellen und die Verfügbarkeit bei Wartungsvorgängen und Hostausfällen aufrechtzuerhalten. Weitere Informationen finden Sie unter vSphere Cluster Design for VMware Cloud Foundation in der VMware Cloud Foundation-Dokumentation.
- Amazon EVS unterstützt die Verwendung einer EC2 Partitionsplatzierungsgruppe oder einer Cluster-Platzierungsgruppe für EC2 Hosts. Die Partitionsplatzierungsgruppe verteilt Ihre EC2 Instances auf logische Partitionen, sodass Gruppen von Instances in einer Partition die zugrunde liegende Hardware nicht mit Gruppen von Instances in verschiedenen Partitionen gemeinsam nutzen. Diese Strategie trägt dazu bei, die Wahrscheinlichkeit korrelierter Hardwareausfälle bei großen verteilten Workloads zu verringern. Cluster-Platzierungsgruppen werden verwendet, um Ihre EC2 Instances innerhalb desselben physischen Racks zu platzieren, um eine geringe Latenz zu gewährleisten. Weitere Informationen finden Sie unter Platzierungsgruppen für Partitionen im Amazon EC2 Benutzerhandbuch.

Weitere Informationen zu AWS Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

VMware Resilienz der Komponenten

Amazon EVS-Kunden sind für die Konfiguration der VMware Komponenten verantwortlich, die auf Amazon EVS ausgeführt werden, um eine hohe Verfügbarkeit Ihrer virtuellen Maschinen (VMs) und die Belastbarkeit Ihrer Workloads sicherzustellen.

Amazon EVS unterstützt die folgenden Resilienzfunktionen der VMware Cloud Foundation (VCF):

- vSphere Replication — Ermöglicht die hostbasierte, asynchrone Replikation Ihrer Daten VMs für Disaster Recovery- und Workload-Migrationszwecke. Weitere Informationen finden Sie unter So funktioniert vSphere Replication in der VMware vSphere Replication-Dokumentation.
- vSAN-Datenschutz — Ermöglicht die schnelle Wiederherstellung nach Betriebsausfällen aufgrund VMs von Ransomware-Angriffen mithilfe systemeigener Snapshots, die lokal auf dem vSAN-Cluster gespeichert sind. Weitere Informationen finden Sie unter Verwenden von vSAN Data Protection in der vSAN-Dokumentation.
- vSphere HA — Bietet automatisches Failover für den VMs Fall eines Hostausfalls. Weitere Informationen finden Sie unter Hochverfügbarkeitsdesign für vCenter Server for VMware Cloud Foundation in der VCF-Dokumentation.

- vSphere Fault Tolerance (FT) — Sorgt für kontinuierliche Verfügbarkeit für geschäftskritische Anwendungen, VMs indem eine weitere virtuelle Maschine erstellt und verwaltet wird, die identisch ist und kontinuierlich verfügbar ist, um sie im Falle einer Failover-Situation zu ersetzen. Weitere Informationen finden Sie in der vSphere-Dokumentation unter So funktioniert Fault Tolerance.
- vSAN Failure to Tolerate (FTT) — Eine vSAN-Einstellung, die festlegt, wie viele Hostausfälle eine VM aushalten kann, bevor sie unzugänglich wird. Dies definiert den Grad der Redundanz und Fehlertoleranz für Ihre virtuellen Maschinen innerhalb des vSAN-Clusters. Weitere Informationen finden Sie unter Tolerieren zusätzlicher Fehler mit Fehlerdomäne im vSAN-Cluster in der vSAN-Dokumentation.

Amazon EVS mit anderen AWS Diensten verwenden

Amazon EVS ist in andere integriert AWS-Services , um zusätzliche Lösungen bereitzustellen. In diesem Thema werden einige der Dienste beschrieben, mit denen Amazon EVS arbeitet, um Funktionen hinzuzufügen.

Themen

- Erstellen Sie Amazon EVS-Ressourcen mit AWS CloudFormation
- Führen Sie Hochleistungs-Workloads mit Amazon FSx for NetApp ONTAP aus

Erstellen Sie Amazon EVS-Ressourcen mit AWS CloudFormation

Amazon EVS ist integriert AWS CloudFormation, ein Service, der Sie bei der Modellierung und Einrichtung Ihrer AWS Ressourcen unterstützt, sodass Sie weniger Zeit mit der Erstellung und Verwaltung Ihrer Ressourcen und Infrastruktur verbringen müssen. Sie erstellen eine Vorlage, die alle gewünschten AWS Ressourcen beschreibt, z. B. eine Amazon EVS-Umgebung, und AWS CloudFormation kümmert sich um die Bereitstellung und Konfiguration dieser Ressourcen für Sie.

Wenn Sie Ihre Vorlage verwenden AWS CloudFormation, können Sie sie wiederverwenden, um Ihre Amazon EVS-Ressourcen konsistent und wiederholt einzurichten. Beschreiben Sie Ihre Ressourcen einfach einmal und stellen Sie dann dieselben Ressourcen immer wieder in mehreren Regionen AWS-Konten bereit.

Amazon EVS und Vorlagen AWS CloudFormation

Um Ressourcen für Amazon EVS und verwandte Services bereitzustellen und zu konfigurieren, müssen Sie AWS CloudFormation Vorlagen verstehen. Vorlagen sind formatierte Textdateien in JSON oder YAML. Diese Vorlagen beschreiben die Ressourcen, die Sie in Ihren AWS CloudFormation Stacks bereitstellen möchten. Wenn Sie mit JSON oder YAML nicht vertraut sind, können Sie AWS CloudFormation Designer verwenden, um Ihnen bei den ersten Schritten mit Vorlagen zu helfen. AWS CloudFormation Weitere Informationen finden Sie unter Was ist AWS CloudFormation Designer? im AWS CloudFormation Benutzerhandbuch.

Amazon EVS unterstützt die Erstellung von Umgebungen in AWS CloudFormation. Weitere Informationen, einschließlich Beispielen für JSON- und YAML-Vorlagen für Ihre Umgebungen, finden Sie in der Amazon EVS-Ressourcentypreferenz im AWS CloudFormation Benutzerhandbuch.

Erfahren Sie mehr über AWS CloudFormation

Weitere Informationen AWS CloudFormation dazu finden Sie in den folgenden Ressourcen:

- AWS CloudFormation
- AWS CloudFormation Benutzerhandbuch
- AWS CloudFormation Benutzerhandbuch für die Befehlszeilenschnittstelle

Führen Sie Hochleistungs-Workloads mit Amazon FSx for NetApp ONTAP aus

Amazon FSx for NetApp ONTAP ist ein Speicherservice, mit dem Sie vollständig verwaltete ONTAP-Dateisysteme in der Cloud starten und ausführen können. NetAppDie Dateisystemtechnologie von ONTAP bietet eine breite Palette von Datenzugriffs- und Datenverwaltungsfunktionen. FSx for ONTAP bietet die Funktionen, die Leistung und die APIs von lokalen NetApp Dateisystemen mit der Agilität, Skalierbarkeit und Einfachheit eines vollständig verwalteten Dienstes. AWS Weitere Informationen finden Sie im Benutzerhandbuch FSx für ONTAP.

Amazon EVS unterstützt die Verwendung von Amazon FSx for NetApp ONTAP als NFS/iSCSI Datenspeicher und als Gastspeicher für VMware virtuelle Maschinen, die auf Amazon EVS ausgeführt werden.

FSx Für NetApp ONTAP als NFS-Datenspeicher konfigurieren

Das folgende Verfahren beschreibt die Mindestschritte, die zur Konfiguration von NetApp ONTAP als NFS-Datenspeicher FSx für Amazon EVS mithilfe der FSx Konsole und der VMware vSphere-Client-Schnittstelle erforderlich sind, die auf Amazon EVS ausgeführt wird.

Voraussetzungen

Bevor Sie Amazon EVS mit Amazon FSx for NetApp ONTAP verwenden, stellen Sie sicher, dass die folgenden erforderlichen Aufgaben abgeschlossen wurden.

- Eine Amazon EVS-Umgebung wird in Ihrer Virtual Private Cloud (VPC) bereitgestellt. Weitere Informationen finden Sie unter Erste Schritte.
- Sie haben Zugriff auf Ihren vSphere-Client, der auf Amazon EVS läuft.

- Sie oder Ihr Speicheradministrator müssen über die erforderlichen Berechtigungen verfügen, um ONTAP-Dateisysteme in Ihrer VPC zu erstellen und zu verwalten FSx . Weitere Informationen finden Sie unter Identitäts- und Zugriffsmanagement für Amazon FSx für NetApp ONTAP.

Ihr IAM-Principal verfügt über die entsprechenden Berechtigungen zum Erstellen und Verwalten von FSx ONTAP-Dateisystemen in Ihrer VPC. Weitere Informationen finden Sie unter the section called “Erstellen und verwalten Sie eine Amazon EVS-Umgebung”.

Erstellen Sie ein Dateisystem FSx für ONTAP NetApp

1. Gehen Sie zur FSx Amazon-Konsole.
2. Wählen Sie Create file system (Dateisystem erstellen) aus.
3. Wählen Sie Amazon FSx für NetApp ONTAP aus.
4. Wählen Sie Weiter aus.
5. Wählen Sie Standard erstellen aus.
6. Wählen Sie als Bereitstellungstyp eine Single-AZ-Bereitstellungsoption aus.

> **Note**
>
> Amazon EVS unterstützt derzeit nur Single-AZ-Bereitstellungen.

7. Geben Sie für SSD-Speicherkapazität 1024 GiB an.
8. Wählen Sie für Durchsatzkapazität die Option Durchsatzkapazität angeben aus. Wählen Sie mindestens 512 MB/s für Single-AZ 1 oder mindestens 768 MB/s für Single-AZ 2.
9. Wählen Sie die Amazon EVS-VPC aus, die Konnektivität zu Ihren Amazon EVS-VLAN-Subnetzen bietet.
10. Wählen Sie eine Sicherheitsgruppe aus, die den gesamten FSx für ONTAP erforderlichen NFS-Datenverkehr zum Amazon VMkernel EVS-Host-Management-VLAN-Subnetz zulässt.
11. Wählen Sie das Amazon EVS Service Access-Subnetz aus, in dem Ihr Dateisystem bereitgestellt werden soll. Weitere Informationen finden Sie unter the section called “Subnetz für den Servicezugriff”.
12. Geben Sie für Junction Path einen aussagekräftigen Namen an, `/vol1` um dieses Volume in vSphere zu identifizieren.
13. Stellen Sie in der Standard-Volume-Konfiguration die Speichereffizienz auf Aktiviert ein.
14. Behalten Sie für die übrigen Einstellungen die Standardwerte bei und wählen Sie Weiter.

15. Überprüfen Sie die Dateisystemattribute und wählen Sie Dateisystem erstellen.

Rufen Sie den NFS-DNS-Namen für die virtuelle Speichermaschine ab

1. Gehen Sie zur FSx Amazon-Konsole.
2. Wählen Sie im linken Menü Dateisysteme aus.
3. Wählen Sie das neu erstellte Dateisystem aus.
4. Wählen Sie die Registerkarte Virtuelle Speichermaschinen aus.
5. Wählen Sie die virtuelle Speichermaschine aus.
6. Wählen Sie die Registerkarte Endpoints aus.
7. Kopieren Sie den DNS-Namen des Netzwerkdateisystems (NFS) für die spätere Verwendung in VMware Vsphere.

Erstellen Sie einen NFS-Datenspeicher in vSphere mithilfe des for ONTAP-Volumes FSx

Folgen Sie den Anweisungen unter Erstellen eines NFS-Datenspeichers in einer vSphere-Umgebung, um Amazon FSx für NetApp ONTAP als externen Speicher für vSphere zu konfigurieren. VMware Verwenden Sie für die Servereinstellung in der vSphere-Client-Schnittstelle den NFS-DNS-Namen der virtuellen Speicher-Maschine (SVM), den Sie im vorherigen Schritt kopiert haben.

FSx Für NetApp ONTAP FSx als iSCSI-Datenspeicher konfigurieren

Das folgende Verfahren beschreibt die Mindestschritte, die zur Konfiguration von NetApp ONTAP als iSCSI-Datenspeicher FSx für Amazon EVS mithilfe der FSx Konsole und der VMware vSphere-Client-Schnittstelle erforderlich sind, die auf Amazon EVS ausgeführt werden.

Voraussetzungen

Bevor Sie Amazon EVS mit Amazon FSx for NetApp ONTAP verwenden, stellen Sie sicher, dass die folgenden erforderlichen Aufgaben abgeschlossen wurden.

- Eine Amazon EVS-Umgebung wird in Ihrer Virtual Private Cloud (VPC) bereitgestellt. Weitere Informationen finden Sie unter Erste Schritte.
- Sie haben Zugriff auf Ihren vSphere-Client, der auf Amazon EVS läuft.

- Sie oder Ihr Speicheradministrator benötigen die erforderlichen Berechtigungen zum Erstellen und Verwalten FSx von ONTAP-Dateisystemen in Ihrer VPC. Weitere Informationen finden Sie unter Identitäts- und Zugriffsmanagement für Amazon FSx für NetApp ONTAP.

Erstellen Sie ein FSx Dateisystem für NetApp ONTAP

1. Gehen Sie zur FSx Amazon-Konsole.
2. Wählen Sie Create file system (Dateisystem erstellen) aus.
3. Wählen Sie Amazon FSx für NetApp ONTAP aus.
4. Wählen Sie Weiter aus.
5. Wählen Sie Standard erstellen aus.
6. Wählen Sie als Bereitstellungstyp eine Single-AZ-Bereitstellungsoption aus.

> **Note**
>
> Amazon EVS unterstützt derzeit nur Single-AZ-Bereitstellungen.

7. Geben Sie für SSD-Speicherkapazität 1024 GiB an.
8. Wählen Sie für Durchsatzkapazität die Option Durchsatzkapazität angeben aus. Wählen Sie mindestens 512 MB/s für Single-AZ 1 oder mindestens 768 MB/s für Single-AZ 2.
9. Wählen Sie die Amazon EVS-VPC aus, die Konnektivität zu Ihren Amazon EVS-VLAN-Subnetzen bietet.
10. Wählen Sie eine Sicherheitsgruppe aus, die den gesamten FSx für ONTAP erforderlichen iSCSI-Verkehr zum Amazon VMkernel EVS-Host-Management-VLAN-Subnetz zulässt.
11. Wählen Sie das Amazon EVS Service Access-Subnetz aus, in dem Ihr Dateisystem bereitgestellt werden soll. Weitere Informationen finden Sie unter the section called “Subnetz für den Servicezugriff”.
12. Stellen Sie in der Standard-Volume-Konfiguration die Speichereffizienz auf Aktiviert ein.
13. Behalten Sie für die übrigen Einstellungen die Standardwerte bei und wählen Sie Weiter.
14. Überprüfen Sie die Dateisystemattribute und wählen Sie Dateisystem erstellen.

Konfigurieren Sie einen Software-iSCSI-Adapter in vSphere für ESX-Hostspeicher

Für jeden ESX-Host müssen Sie den Software-iSCSI-Adapter so konfigurieren, dass Ihre ESX-Hosts ihn für den Zugriff auf iSCSI-Speicher verwenden können. Anweisungen zur Konfiguration des Software-iSCSI-Adapters für ESX-Hosts in vSphere finden Sie unter Hinzufügen oder Entfernen des Software-iSCSI-Adapters in der VMware vSphere-Produktdokumentation.

Nachdem Sie den Software-iSCSI-Adapter konfiguriert haben, kopieren Sie den iSCSI Qualified Name (IQN), der einem iSCSI-Adapter zugeordnet ist. Diese Werte werden später verwendet.

Eine iSCSI-LUN erstellen

FSx for ONTAP ermöglicht es Ihnen, Logical Unit Numbers (LUNs) zu erstellen, die speziell für den iSCSI-Zugriff vorgesehen sind und Ihren ESX-Hosts gemeinsamen Blockspeicher zur Verfügung stellen. Sie verwenden die NetApp ONTAP CLI, um eine LUN zu erstellen.

Im Folgenden finden Sie einen Beispielbefehl.

> **Note**
>
> Es wird empfohlen, die LUN-Größe auf 90% der Volume-Größe zu konfigurieren.

```
lun create -vserver <your_svm_name> \
-path /vol/<your_volume_name>/<lun_name> \
-size <required_datastore_capacity> \
-ostype vmware
```

Weitere Informationen finden Sie unter Erstellen einer iSCSI-LUN im Benutzerhandbuch FSx für ONTAP.

Konfiguration und Zuordnung einer Initiatorgruppe zur iSCSI-LUN

Nachdem Sie eine iSCSI-LUN erstellt haben, besteht der nächste Schritt im Prozess darin, eine Initiatorgruppe (`igroup`) zu erstellen, um das Volume mit dem Cluster zu verbinden und die LUN der Initiatorgruppe zuzuordnen. Sie verwenden die NetApp ONTAP CLI, um diese Aktionen durchzuführen.

1. Konfigurieren Sie die Initiatorgruppe.

Im Folgenden finden Sie einen Beispielbefehl. Verwenden Sie für `--initiator` den iSCSI-Adapter IQNs , den Sie im vorherigen Schritt kopiert haben.

```
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. Vergewissern Sie sich, dass der `igroup` vorhanden ist.

```
lun igroup show
```

3. Ordnen Sie die LUN der Initiatorgruppe zu. Im Folgenden finden Sie einen Beispielbefehl.

```
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. Verwenden Sie den `lun show -path` Befehl, um zu bestätigen, dass die LUN erstellt, online und zugeordnet wurde.

```
lun show -path /vol/<vol_name>/<lun_name> -fields state,mapped,serial-hex
```

Weitere Informationen finden Sie unter Provisioning iSCSI for Linux oder Provisioning iSCSI for Windows im for ONTAP User FSx Guide.

Konfigurieren Sie die dynamische Erkennung der iSCSI-LUN in vSphere

Damit die ESX-Hosts die iSCSI-LUN sehen können, müssen Sie die dynamische Erkennung für jeden Host in der vSphere-Client-Schnittstelle konfigurieren. Geben Sie für das Feld iSCSI-Server den (NFS-) DNS-Namen ein, den Sie im vorherigen Schritt kopiert haben. Weitere Informationen finden Sie unter Konfigurieren von dynamischer oder statischer Erkennung für iSCSI und iSER auf dem ESX-Host in der VMware vSphere-Produktdokumentation.

Erstellen Sie einen VMFS-Datenspeicher in VMware vSphere mithilfe der iSCSI-LUN

VMFS-Datenspeicher (Virtual Machine File System) dienen als Repositorys für virtuelle Maschinen. VMware Folgen Sie den Anweisungen unter Erstellen eines vSphere VMFS-Datenspeichers, um den VMFS-Datenspeicher in VMware vSphere mithilfe der zuvor konfigurierten iSCSI-LUN einzurichten.

Fehlerbehebung

In diesem Kapitel werden einige häufig auftretende Probleme bei der Erstellung oder Verwaltung von Amazon EVS-Umgebungen beschrieben.

Hinweise zu Broadcom und AWS Support

AWS bietet Unterstützung für Amazon EVS und die zugehörigen Infrastrukturdienste, einschließlich VMware Cloud Foundation (VCF). Für VCF-spezifische Konfigurationsanleitungen oder Probleme im Zusammenhang mit anderen VMware Produkten wie Aria Suite, HCX oder NSX können Sie sich mit Ihrem Broadcom-Supportanspruch auch direkt an Broadcom wenden. Weitere Informationen finden Sie im Broadcom Support Portal.

Beheben Sie fehlgeschlagene Umgebungsstatusprüfungen

Amazon EVS führt automatische Prüfungen Ihrer Umgebung durch, um Probleme zu identifizieren. Sie können den Status Ihrer Umgebung anzeigen, um spezifische und erkennbare Probleme zu identifizieren.

Überprüfen Sie die Informationen zur Überprüfung des Umgebungsstatus

Um beeinträchtigte Umgebungen mit der Amazon EVS-Konsole zu untersuchen

1. Öffnen Sie die Amazon EVS-Konsole.
2. Wählen Sie im Navigationsbereich Umgebungen und dann Ihre Umgebung aus.
3. Wählen Sie die Registerkarte Details aus, um einen Überblick über die Umgebung zu erhalten.
4. Überprüfen Sie den Status der Umgebung. Bewegen Sie den Mauszeiger auf dieses Feld, um ein Popover mit individuellen Ergebnissen für jede Überprüfung des Umgebungsstatus zu öffnen.

Die Erreichbarkeitsprüfung ist fehlgeschlagen

Die Erreichbarkeitsprüfung bestätigt, dass Amazon EVS über eine dauerhafte Verbindung zu SDDC Manager verfügt. Wenn Amazon EVS die Umgebung nicht erreichen kann, schlägt diese Prüfung fehl.

Schlägt diese Prüfung fehl, kann Amazon EVS SDDC Manager nicht mehr erreichen, um den Umgebungsstatus zu überprüfen, und der Umgebung können keine Hosts mehr hinzugefügt werden.

Ein Fehler bei der Erreichbarkeit führt auch dazu, dass die Wiederverwendung des Lizenzschlüssels und die Überprüfung der Schlüsselabdeckung fehlschlagen und die Überprüfung der Anzahl der Hosts die Antwort Unbekannt zurückgibt.

Um die Erreichbarkeit sicherzustellen, überprüfen Sie Folgendes:

- Stellen Sie sicher, dass Ihre Zertifikate gültig und nicht abgelaufen sind. Sie können die SDDC-Manager-Benutzeroberfläche oder den vSphere-Client verwenden, um Zertifikate in einer VCF-Umgebung zu verwalten. Nach der Bereitstellung wird empfohlen, alle Zertifikate der VMware Cloud Foundation-Verwaltungsdomäne zu ersetzen. Weitere Informationen finden Sie unter Zertifikate in VMware Cloud Foundation verwalten in der VMware Cloud Foundation-Dokumentation.
- Stellen Sie sicher, dass Ihre DNS-Server vom Dienstzugriffssubnetz aus erreichbar sind, dass die DNS-Einträge gültig sind und keine doppelten Hostnamen oder IP-Adressen vorhanden sind.
- Wenn Sie Ihre eigenen Firewallregeln erstellen möchten, folgen Sie diesen Richtlinien:
  - Erlauben Sie TCP/UDP den Zugriff auf die DNS-Server.
  - HTTPS/SSH Erlaubt den Zugriff auf das VLAN-Subnetz für die Hostverwaltung.
  - Erlaubt HTTPS/SSH den Zugriff auf das VLAN-Subnetz der Management-VM.

Wenn Sie das Problem nach Befolgung dieser Anleitung immer noch nicht lösen können, empfehlen wir Ihnen, sich an den Support zu wenden, um weitere AWS Unterstützung zu erhalten.

Die Überprüfung der Hostanzahl ist fehlgeschlagen

Diese Prüfung stellt sicher, dass Ihre Umgebung über mindestens vier Hosts verfügt. Dies ist eine Voraussetzung für VCF 5.2.x.

Schlägt diese Prüfung fehl, müssen Sie Hosts hinzufügen, damit Ihre Umgebung diese Mindestanforderung erfüllt. Amazon EVS unterstützt nur Umgebungen mit 4 bis 16 Hosts.

Die Überprüfung der Wiederverwendung von Schlüsseln ist fehlgeschlagen

Diese Prüfung stellt sicher, dass der VCF-Lizenzschlüssel nicht von einer anderen Amazon EVS-Umgebung verwendet wird. VCF-Lizenzen können nur für eine Amazon-EVS-Umgebung verwendet werden. Diese Prüfung schlägt fehl, wenn Sie in einer Anfrage zur Umgebungserstellung VCF-Lizenzschlüssel angeben, die bereits von einer anderen Umgebung verwendet werden.

Schlägt diese Prüfung fehl, erhalten Sie die Fehlermeldung, dass die Amazon-EVS-Umgebung nicht erstellt werden konnte. Um das Problem zu beheben, überprüfen Sie Ihre Lizenzeinstellungen in SDDC Manager und ersetzen Sie alle zuvor verwendeten Lizenzen durch nicht verwendete Lizenzen.

> **Important**
>
> Verwenden Sie die SDDC Manager-Benutzeroberfläche, um die VCF-Lösung und die vSAN-Lizenzschlüssel zu verwalten. Amazon EVS erfordert, dass Sie gültige VCF-Lösungs- und vSAN-Lizenzschlüssel im SDDC Manager verwalten, damit der Service ordnungsgemäß funktioniert. Schlüssel müssen Ihren Hosts und dem vSAN-Cluster zwar mithilfe des vSphere Client zugewiesen werden, Sie müssen jedoch sicherstellen, dass diese Schlüssel auch auf dem Lizenzierungsbildschirm der SDDC Manager-Benutzeroberfläche angezeigt werden.

Die Überprüfung der Schlüsselabdeckung ist fehlgeschlagen

Bei dieser Prüfung wird überprüft, ob Ihr vCenter Server zugewiesener VCF-Lizenzschlüssel ausreichend vCPU-Kerne und vSAN-Speicherkapazität (TiB) für alle bereitgestellten Hosts zuweist.

Schlägt diese Prüfung fehl, erhalten Sie die Fehlermeldung, dass die Amazon-EVS-Umgebung nicht erstellt werden konnte. Ein Ausfall der Schlüsselabdeckung kann auf eines der folgenden Probleme hinweisen:

- VCF-Lizenzen sind vCenter Server nicht ordnungsgemäß zugewiesen. Sie müssen vCenter Server eine Lizenz zuweisen, bevor der Testzeitraum oder die aktuell zugewiesene Lizenz abläuft. Wenn dies das Problem ist, überprüfen Sie die Lizenzzuweisungen in SDDC Manager.
- Aktuelle VCF-Lizenzen decken den Bedarf an vCPU-Kern und vSAN-Speicherkapazität nicht ab. Die Anforderungen für den VCF-Lösungsschlüssel (einschließlich der Mindestanzahl an Kernen) und den vSAN-Lizenzschlüssel (einschließlich vSAN-Mindestkapazität) variieren je nach Instanztyp. Spezifische Schwellenwerte für Ihre Konfiguration finden Sie unter. the section called “VCF-Abonnements” Ist dies das Problem, fügen Sie vSAN-Lizenzen in SDDC Manager hinzu, bis Ihre Verwendungsanforderungen erfüllt sind.

Wenn das Problem mit den oben genannten Maßnahmen nicht behoben werden kann, wenden Sie sich an den AWS Support, um weitere Unterstützung zu erhalten.

> **Important**
>
> Verwenden Sie die SDDC Manager-Benutzeroberfläche, um die VCF-Lösung und die vSAN-Lizenzschlüssel zu verwalten. Amazon EVS erfordert, dass Sie gültige VCF-Lösungs- und vSAN-Lizenzschlüssel im SDDC Manager verwalten, damit der Service ordnungsgemäß funktioniert. Schlüssel müssen Ihren Hosts und dem vSAN-Cluster zwar mithilfe des vSphere Client zugewiesen werden, Sie müssen jedoch sicherstellen, dass diese Schlüssel auch auf dem Lizenzierungsbildschirm der SDDC Manager-Benutzeroberfläche angezeigt werden.

Der vSphere HA-Agent auf diesem Host konnte die Isolationsadresse nicht erreichen

Auf der vCenter-Benutzeroberfläche wird bei ausgewähltem ESX-Host die Meldung „Der vSphere HA-Agent auf diesem Host konnte die Isolationsadresse < IPv6 address> nicht erreichen“ angezeigt.

Diese Fehlermeldung weist darauf hin, dass der vSphere HA-Agent auf einem Host die IPv6 Standard-Isolationsadresse, die vSphere HA für Heartbeat-Prüfungen verwendet, nicht erreichen kann. Die Fehlermeldung weist nicht auf ein Problem hin und tritt nur auf, weil Amazon EVS derzeit keine Unterstützung IPv6 bietet. Das Fehlen von IPV6 Unterstützung für Amazon EVS hat keinen Einfluss auf die Kernfunktionalität von vSphere HA.

vSAN-Upgrade-Vorprüfungen schlagen für ESX-Hostcluster fehl

Beim Versuch, den ESX-Hostcluster mit SDDC Manager zu aktualisieren, schlagen vSAN-Festplatten-bezogene Vorprüfungen möglicherweise fehl. Dies liegt daran, dass Amazon EVS vSAN Express Storage Architecture (ESA) verwendet und die Upgrade-Vorabprüfungen nicht für vSAN ESA gelten. Weitere Informationen finden Sie im Broadcom-Knowledgebase-Artikel zu diesem Thema.

Fehler beim Hinzufügen eines Hosts aufgrund eines inkompatiblen Cluster-Images

Problem

Wenn Sie Ihrer Umgebung einen Host hinzufügen, verfügt der Host über die neueste verfügbare Version des benutzerdefinierten EVS-Add-ons. Wenn Ihre Umgebung Hosts mit einer älteren Add-

On-Version verwendet, schlägt das Hinzufügen neuer Hosts fehl und es wird die Fehlermeldung angezeigt, dass der neue Host nicht mit Ihrem Cluster-Image kompatibel ist. Um dieses Problem zu beheben, müssen Sie vSphere Lifecyle Manager verwenden, um die neueste verfügbare Add-On-Version vom neu hinzugefügten Host zu extrahieren.

Lösung

Dazu gehen Sie wie folgt vor:

1. Gehen Sie zum Inventar für Hosts und Cluster in VMware vCenter Server.
2. Extrahieren Sie das Add-On aus dem neu hinzugefügten Host, indem Sie einen temporären leeren Cluster erstellen.
3. Wählen Sie unter Grundlagen die Option Image von einem vorhandenen Host im vCenter-Inventar importieren aus und erstellen Sie den Cluster. Behalten Sie alle anderen Einstellungen als Standard bei.
4. Sobald dieser temporäre Cluster mit dem extrahierten Image erstellt wurde, können Sie den temporären Cluster löschen. Das Add-on ist jetzt in Ihrem vSphere Lifecycle Manager-Depot verfügbar.
5. Gehen Sie zu Ihrem Umgebungscluster und wählen Sie die Registerkarte Updates aus.
6. Bearbeiten Sie Ihr Cluster-Image und ändern Sie die Add-On-Version auf die neu extrahierte Version.
7. Wählen Sie Speichern.
8. Versuchen Sie im SDDC Manager erneut, die fehlgeschlagene Aufgabe zum Hinzufügen von Hosts auszuführen. Dadurch werden Ihre Cluster-Hosts standardisiert und alle Hosts auf die neueste Add-On-Version aktualisiert. Für die Wiederherstellung von Cluster-Images sind Neustarts der Hosts erforderlich.

SDDC Manager schlägt die VCF-Hostvalidierung bei der Host-Inbetriebnahme fehl

Problem

Wenn Sie Ihre ESX-Version nach der Bereitstellung der Amazon EVS-Umgebung aktualisiert haben, schlägt der SDDC-Manager möglicherweise bei der VCF-Host-Validierung im Schritt Provision-Hosts fehl. Um dieses Problem zu beheben, müssen Sie vSphere Lifecyle Manager verwenden, um ESX auf dem neu hinzugefügten Host zu aktualisieren.

Lösung

Dazu gehen Sie wie folgt vor:

> **Important**
>
> Diese Schritte erfordern das vorübergehende Hinzufügen des Hosts zu vCenter außerhalb von SDDC Manager. Wenn Sie vSphere Lifecyle Manager für andere Operationen als ESX-Upgrades verwenden, kann Ihr Host möglicherweise unbrauchbar werden und Sie müssen einen neuen Amazon EVS-Host löschen und erstellen.

1. Gehen Sie zum Inventar für Hosts und Cluster in VMware vCenter Server.
2. Fügen Sie den Host vorübergehend zu Ihrem virtuellen Rechenzentrum hinzu und achten Sie darauf, dass Sie „Host mit Image verwalten“ auswählen. Der Host wird in einem späteren Schritt entfernt, nachdem das ESX-Upgrade abgeschlossen ist. Weitere Informationen finden Sie in der vSphere-Dokumentation unter Hinzufügen eines Hosts zu Ihrem vSphere-Rechenzentrum oder -Ordner.
3. Sobald der Host zu vSphere hinzugefügt wurde, führen Sie ein Upgrade der ESX-Version auf dem Host durch. Dies kann auf der Registerkarte Updates Ihres Hosts erfolgen. Bearbeiten Sie das Host-Image so, dass es der ESX-Version Ihres Clusters entspricht.
4. Nachdem das Upgrade abgeschlossen ist, entfernen Sie den Host aus Ihrem vCenter-Inventar. Weitere Informationen finden Sie unter So entfernen Sie einen ESX-Host aus Ihrer vCenter Server-Instanz in der vSphere-Dokumentation.
5. Nehmen Sie Ihren Host im SDDC Manager in Betrieb. Weitere Informationen finden Sie unter Commission Hosts in der VMware Cloud Foundation-Dokumentation.
6. Nachdem der Host in Betrieb genommen wurde, fügen Sie den Host mithilfe von SDDC Manager zu Ihrem Cluster hinzu.

Der Windows Server-Berechtigungsstatus ist aufgrund eines Fehlers bei der Erreichbarkeit der Appliance gefährdet

Eine Berechtigung geht in den Risikostatus über, wenn der zugehörige Amazon EVS-Connector die Erreichbarkeitsprüfung für die VCF-Verwaltungs-Appliance nicht besteht. Bei Windows Server-Berechtigungen haben Sie ab dem Zeitpunkt, an dem die Berechtigung den Status „Gefährdet“

erreicht hat, 8 Stunden Zeit, um die Verbindung wiederherzustellen. Wenn die Verbindung innerhalb dieses Zeitraums nicht wiederhergestellt wird, werden die Berechtigungen automatisch gelöscht und die Windows Server-Nutzungsverfolgung wird gestoppt.

Überprüfen Sie Folgendes, um dieses Problem zu beheben:

- Stellen Sie sicher, dass der Connector-Status Aktiv und der Status der Erreichbarkeitsprüfung Fehlgeschlagen ist.
- Stellen Sie sicher, dass die in AWS Secrets Manager gespeicherten Appliance-Anmeldeinformationen aktuell und korrekt sind. Wenn die Anmeldeinformationen in der Appliance rotiert wurden, aktualisieren Sie die Werte im vorhandenen Secrets Manager Manager-Secret. Wenn Sie auf ein anderes Geheimnis verweisen müssen, verwenden Sie es, UpdateEnvironmentConnector um den geheimen Bezeichner zu aktualisieren.
- Stellen Sie sicher, dass Ihre DNS-Server vom Dienstzugriffssubnetz aus erreichbar sind, dass die DNS-Einträge für den FQDN der Appliance gültig sind und dass keine doppelten Hostnamen oder IP-Adressen vorhanden sind.
- Stellen Sie sicher, dass die Firewallregeln den HTTPS/SSH Zugriff auf das VLAN-Subnetz der Management-VM und TCP/UDP den Zugriff auf DNS-Server zulassen.
- Stellen Sie sicher, dass die Appliance läuft und darauf zugegriffen werden kann.

Sobald die Verbindung wiederhergestellt ist, kehren die Berechtigungen automatisch in den fehlerfreien Status Created zurück. Wenn Berechtigungen bereits gelöscht wurden und den Status „Berechtigung entfernt“ haben, müssen Sie neue Berechtigungen erstellen, nachdem der Connector in den Status Aktiv zurückgekehrt ist und die Erreichbarkeitsprüfung bestanden wurde.

Wenn Sie das Problem nach Befolgung dieser Anleitung immer noch nicht lösen können, empfehlen wir Ihnen, sich an den Support zu wenden, um weitere AWS Unterstützung zu erhalten.

Der Anspruch ist fehlgeschlagen, weil das Gastbetriebssystem nicht unterstützt wird

Eine Berechtigungserstellung schlägt fehl oder eine bestehende Berechtigung wird entfernt, wenn Amazon EVS feststellt, dass auf der VM ein Gastbetriebssystem ausgeführt wird, das für die Amazon EVS Windows Server-Lizenzierung nicht unterstützt wird.

Dies kann auftreten, wenn:

- Eine VM mit einer bestehenden Windows Server-Berechtigung wird neu konfiguriert, sodass sie eine nicht unterstützte Betriebssystemversion oder ein anderes Betriebssystem als Windows verwendet.
- Eine Berechtigungserstellung ist fehlgeschlagen, weil auf einer VM bereits ein Gastbetriebssystem ausgeführt wird, das nicht unterstützt wird.

So beheben Sie dieses Problem

- Stellen Sie sicher, dass der Connector-Status Aktiv und der Status der Erreichbarkeitsprüfung Bestanden lautet.
- Überprüfen Sie, ob das auf der VM konfigurierte Gastbetriebssystem konfiguriert ist. Die Amazon EVS Windows Server-Lizenzierung unterstützt Windows Server 2016 oder höher.
- Konfigurieren Sie die VM neu, um eine unterstützte Windows Server-Version zu verwenden.
- Erstellen Sie nach der Aktualisierung des Gastbetriebssystems eine neue Berechtigung für die VM.
- (Optional) Löschen Sie die Berechtigung mit dem Status „Berechtigung entfernt“.

Wenn Sie das Problem nach Befolgung dieser Anleitung immer noch nicht lösen können, empfehlen wir Ihnen, sich an den Support zu wenden, um weitere AWS Unterstützung zu erhalten.

Der Anspruchsstatus lautet „Anspruch entfernt“

Eine Berechtigung mit dem Status „Berechtigung entfernt“ bedeutet, dass Amazon EVS die Berechtigung für die VM entfernt hat. Wenn eine Berechtigung entfernt wird, wird die Windows Server-Nutzungsverfolgung für die betroffene VM beendet.

Dieser Status kann verschiedene Ursachen haben:

- Erreichbarkeitsfehler der Appliance, bei dem die Übergangsfrist von 8 Stunden überschritten wurde. Siehe the section called “Der Windows Server-Berechtigungsstatus ist aufgrund eines Fehlers bei der Erreichbarkeit der Appliance gefährdet”.
- VM ist nicht mehr im Geräteinventar vorhanden. Siehe the section called “Die Berechtigung wurde entfernt, weil die virtuelle Maschine getrennt, isoliert oder nicht im Inventar enthalten ist”.
- Die virtuelle Maschine wurde von ihrem Host getrennt oder isoliert. Siehe the section called “Die Berechtigung wurde entfernt, weil die virtuelle Maschine getrennt, isoliert oder nicht im Inventar enthalten ist”.

- Das VM-Gastbetriebssystem wurde auf eine nicht unterstützte Version geändert. Siehe the section called “Der Anspruch ist fehlgeschlagen, weil das Gastbetriebssystem nicht unterstützt wird”.

So stellen Sie die Berechtigung wieder her:

- Überprüfen Sie die Fehlerdetails der Berechtigung, um die genaue Ursache für die Entfernung zu ermitteln.
- Beheben Sie das zugrundeliegende Problem.
- Erstellen Sie eine neue Berechtigung für die VM, sobald sich der Connector im Status Aktiv befindet und eine Erreichbarkeitsprüfung im Status Bestanden durchgeführt wurde.
- (Optional) Löschen Sie die Berechtigung mit dem Status „Berechtigung entfernt“.

Wenn Sie das Problem nach Befolgung dieser Anleitung immer noch nicht lösen können, empfehlen wir Ihnen, sich an den Support zu wenden, um weitere AWS Unterstützung zu erhalten.

Die Berechtigung wurde entfernt, weil die virtuelle Maschine getrennt, isoliert oder nicht im Inventar enthalten ist

Eine Berechtigung wird entfernt, wenn Amazon EVS feststellt, dass eine VM getrennt oder isoliert wurde oder nicht mehr im Appliance-Inventar vorhanden ist. Die Berechtigung wird sofort entfernt und die Nutzungsverfolgung wird gestoppt.

So beheben Sie dieses Problem

- Stellen Sie sicher, dass der Connector-Status Aktiv und der Status der Erreichbarkeitsprüfung Bestanden lautet.
- Überprüfen Sie den Verbindungsstatus der VM in Ihrer Appliance. Eine getrennte oder isolierte VM kann auf ein Host- oder Netzwerkproblem hinweisen.
- Beheben Sie das zugrunde liegende Host- oder Netzwerkproblem, das dazu führt, dass die virtuelle Maschine getrennt oder isoliert wurde.
- Nachdem die virtuelle Maschine wieder verbunden ist und normal läuft, erstellen Sie eine neue Berechtigung, um die Nutzung von Windows Server wieder aufzunehmen.

Wenn Sie das Problem nach Befolgung dieser Anleitung immer noch nicht lösen können, empfehlen wir Ihnen, sich an den Support zu wenden, um weitere AWS Unterstützung zu erhalten.

Protokollieren von Amazon EVS-API-Aufrufen mit AWS CloudTrail

Amazon EVS ist in einen Service integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem IAM-Benutzer, einer IAM-Rolle oder einem AWS Service in Amazon EVS ausgeführt wurden. CloudTrail erfasst alle AWS API-Aufrufe für Amazon EVS als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der Amazon EVS-Konsole und Code-Aufrufe der Amazon EVS-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für Amazon EVS. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen. Anhand der von gesammelten Informationen können Sie die Anfrage CloudTrail, die an Amazon EVS gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch.

> **Note**
>
> Amazon EVS protokolliert keine Benutzeraktivitäten für AWS Nichtkomponenten, wie z. B. Aktivitäten in Ihrer VCF-Umgebung. Diese Aktivitäten werden in verschiedenen VMware Konsolen wie vSphere und NSX Manager protokolliert.
> Wenn eine zentralisierte VCF-Protokollierung gewünscht wird, können Sie VCF-Überwachungslösungen wie VMware Cloud Foundation Operations konfigurieren, um dieses Ergebnis zu erzielen.

Amazon EVS-Informationen in CloudTrail

CloudTrail ist für Ihr AWS Konto aktiviert, wenn Sie das Konto erstellen. Wenn eine Aktivität in Amazon EVS auftritt, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen in der CloudTrail Ereignishistorie in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem AWS Konto ansehen, suchen und herunterladen. Weitere Informationen finden Sie unter Ereignisse mit CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung von Ereignissen in Ihrem AWS Konto, einschließlich Ereignissen für Amazon EVS, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von

Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole erstellen, gilt der Trail standardmäßig für alle AWS Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- CloudTrail unterstützte Dienste und Integrationen
- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen
- Empfangen von CloudTrail Protokolldateien von mehreren Konten

Alle Amazon EVS-Aktionen werden von der Amazon EVS API-Referenz protokolliert CloudTrail und sind in dieser dokumentiert. Beispielsweise generieren Aufrufe von `GetEnvironment` und `DeleteEnvironment` Aktionen Einträge in den CloudTrail Protokolldateien. `CreateEnvironment`

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM) - Benutzeranmeldedaten gestellt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

Grundlegendes zu Amazon EVS-Protokolldateieinträgen

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Amazon EVS-Servicekontingente

Amazon EVS ist in Service Quotas integriert, AWS-Service sodass Sie Ihre Kontingente von einem zentralen Ort aus einsehen und verwalten können. Weitere Informationen zu Service Quotas finden Sie unter Was sind Service Quotas im Benutzerhandbuch für Service Quotas.

Mit der Integration von Service Quotas können Sie das AWS-Managementkonsole oder verwenden, AWS CLI um den Wert Ihrer Amazon EVS-Kontingente nachzuschlagen und eine Kontingenterhöhung für anpassbare Kontingente zu beantragen. Weitere Informationen finden Sie unter Beantragung einer Kontingenterhöhung im Service Quotas Quota-Benutzerhandbuch und request-service-quota-increasein der AWS CLI Befehlsreferenz.

Weitere Informationen zu Amazon EVS-Servicekontingenten finden Sie unter Amazon EVS-Kontingente im AWS Allgemeinen Referenzhandbuch.

Important

Stellen Sie sicher, dass Ihr EC2 Running On-Demand-Standard-Instance-Kontingent der Anzahl der vCPUs entspricht, die Sie für alle EC2-Instances benötigen, die Sie auf Amazon EVS verwenden werden. Informationen zur Erhöhung der EC2-Servicekontingenten finden Sie unter Erhöhung beantragen im Amazon EC2 EC2-Benutzerhandbuch.

Note

Wenn Sie planen, EC2 Dedicated Hosts für Ihre Amazon EVS-Umgebung zu verwenden, stellen Sie sicher, dass Ihr EC2 Dedicated Hosts-Kontingent die Anzahl der Dedicated Hosts widerspiegelt, die Sie für eine gewünschte Region verwenden möchten. Informationen zur Erhöhung der EC2-Servicekontingenten finden Sie unter Erhöhung beantragen im Amazon EC2 EC2-Benutzerhandbuch.

Note

Wenn Sie die HCX-Internetverbindung konfigurieren, muss Ihr IPAM-Kontingent für die von Amazon bereitgestellte Länge der zusammenhängenden öffentlichen IPv4 CIDR-

Blocknetzmaske /28 oder höher sein. Weitere Informationen finden Sie unter Kontingente für Ihr IPAM.

> **Note**
>
> Amazon CloudWatch sammelt AWS Nutzungsmetriken für Amazon EVS-Ressourcen, für die Kontingente gelten (Umgebung und Hosts). Weitere Informationen finden Sie unter CloudWatch Nutzungsmetriken im CloudWatch Amazon-Benutzerhandbuch.

Amazon EVS-Servicekontingente finden Sie in der AWS-Managementkonsole

1. Öffnen Sie die Service Quotas-Konsole.
2. Wählen Sie im linken Navigationsbereich AWS Services aus.
3. Suchen Sie in der AWS Serviceliste nach Amazon Elastic VMware Service und wählen Sie es aus.
4. Wählen Sie Kontingente anzeigen aus.

   In der Liste der Service-Kontingente finden Sie den Namen des Service-Kontingents, den angewendeten Wert (falls verfügbar), das AWS Standardkontingent und ob der Kontingentwert anpassbar ist.
5. Wählen Sie den Kontingentnamen, um zusätzliche Informationen zu einem Service Quota anzuzeigen, z. B. seine Beschreibung.
6. (Optional) Um eine Kontingenterhöhung anzufordern, wählen Sie das Kontingent aus, das Sie erhöhen möchten, wählen Sie Erhöhung auf Kontoebene beantragen aus, geben Sie die erforderlichen Informationen ein oder wählen Sie sie aus und wählen Sie Anfrage aus.

Weitere Informationen zum Umgang mit Servicekontingenten mithilfe von finden Sie im Service Quotas User Guide. AWS-Managementkonsole Informationen zum Beantragen einer Kontingenterhöhung finden Sie unter Beantragen einer Kontingenterhöhung im Service-Quotas-Benutzerhandbuch.

Amazon EVS-Servicekontingente mit der AWS CLI anzeigen

Führen Sie den folgenden Befehl aus, um Ihre Amazon EVS-Kontingente anzuzeigen.

```
aws service-quotas list-aws-default-service-quotas \
    --query 'Quotas[*].
{Adjustable:Adjustable,Name:QuotaName,Value:Value,Code:QuotaCode}' \
    --service-code evs \
    --output table
```

> **Note**
>
> Das zurückgegebene Kontingent ist die Anzahl der Amazon EVS-Umgebungen oder Hosts, die in diesem Konto in der aktuellen AWS Region erstellt werden können.

Weitere Informationen zum Arbeiten mit Servicekontingenten mithilfe der AWS CLI finden Sie unter service-quota in der AWS CLI-Befehlsreferenz. Informationen zum Anfordern einer Erhöhung des Kontingents finden Sie unter dem request-service-quota-increaseBefehl in der AWS CLI-Befehlsreferenz.

Dokumentenverlauf für das Amazon Elastic VMware Service User Guide

In der folgenden Tabelle werden die Dokumentationsversionen für Amazon Elastic VMware Service beschrieben.

Änderung	Beschreibung	Datum
Unterstützung für den Instance-Typ hinzugefügt	Amazon EVS unterstützt jetzt den Instance-Typ i7i.metal -24xl für die Verwendung mit VMware Cloud Foundation (VCF) -Umgebungen. Dieser Bare-Metal-Instanc e-Typ ist in allen Cloud Foundation (VCF) -Versionen verfügbar. VMware	27. April 2026
Benutzeranleitungen für Environment Connector und Berechtigungen wurden hinzugefügt	Es wurden Benutzerh andbücher für die Verwaltun g von Konnektoren und Berechtigungen für die Amazon EVS-Umgebung hinzugefügt. Konnektor en stellen eine dauerhafte Verbindung zwischen Amazon EVS und einer VCF-Appli ance her und ermöglichen so Funktionen wie Windows-L izenz inklusive. Mit Berechtig ungen können Sie den Windows Server-Lizenzschut z für virtuelle Maschinen in Ihrer Amazon EVS-Umgebung aktivieren oder entfernen.	20. April 2026

Amazon aktualisiert EVSService RolePolicy	Amazon EVS hat die verwaltete Richtlinie aktualisiertAmazonEVSServiceRolePolicy , sodass der Service vCenter-Anmeldeinformationen von AWS Secrets Manager abrufen und mit vom Kunden verwalteten KMS-Schlüsseln verschlüsselte Geheimnisse entschlüsseln kann.	23. März 2026
Versionsunterstützung für VCF-5.2.2	Amazon EVS unterstützt jetzt VCF-5.2.2, sodass Sie bei der Einrichtung Ihrer EVS-Umgebungen und Hosts unterstützte Kombinationen von VMware Cloud Foundation (VCF) - und ESX-Softwareversionen angeben können.	20. Januar 2026
Amazon EVS in mehreren AWS Regionen veröffentlicht	Amazon EVS wurde in den Regionen USA West (Nordkalifornien), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Kanada West (Calgary), Europa (Mailand), Mexiko (Zentral) und Südamerika (São Paulo) veröffentlicht.	15. Dezember 2025
Amazon EVS in mehreren AWS Regionen veröffentlicht	Amazon EVS wurde in den Regionen Asien-Pazifik (Mumbai), Asien-Pazifik (Sydney), Kanada (Zentral) und Europa (Paris) veröffentlicht.	6. November 2025

Amazon EVS in den Regionen Asien-Pazifik (Singapur) und Europa (London) veröffentlicht	Amazon EVS wurde in den Regionen Asien-Pazifik (Singapur) und Europa (London) veröffentlicht.	30. September 2025
Amazon EVS unterstützt die HCX-Migration über das öffentliche Internet	Amazon EVS ermöglicht Ihnen jetzt die sichere Migration und Erweiterung Ihrer Layer-2-Netzwerke von Ihren lokalen Rechenzentren zu Amazon EVS-Umgebungen über das öffentliche Internet.	18. September 2025
Amazon aktualisiert EVSService RolePolicy	Amazon EVS hat die verwaltete Richtlinie aktualisiertAmazonEVSServiceRolePolicy , um umfassende Ressourcenverwaltungsfunktionen wie EC2-Instance-Management, EBS-Volumenoperationen und AWS Secrets Manager Manager-Integration hinzuzufügen. Weitere Informationen finden Sie unter Amazon EVS-Updates für AWS verwaltete Richtlinien.	14. August 2025
Amazon aktualisiert EVSService RolePolicy	Die AWS verwaltete Richtlinie Amazon wurde aktualisiert EVSServiceRolePolicy.	4. August 2025

Die Anzahl der Umgebungen pro AWS Kontingent wurde veröffentlicht	Anzahl der von Amazon EVS veröffentlichten Umgebungen pro AWS Kontingent. Die Anzahl der Umgebungen pro AWS Kontingent stellt die maximale Anzahl von Amazon EVS-Umgebungen dar, die in einem bestimmten Konto und einer bestimmten Region erstellt werden können.	8. Juli 2025
Amazon EVS in der Region Europa (Irland) veröffentlicht	Amazon EVS wurde in der Region Europa (Irland) veröffentlicht.	18. Juni 2025
Amazon veröffentlicht EVSService RolePolicy	Die AWS verwaltete Richtlinie Amazon EVSService RolePolicy wurde veröffentlicht.	9. Juni 2025
Erste Veröffentlichung des Benutzerhandbuchs	Das Amazon Elastic VMware Service User Guide wurde veröffentlicht. Das Amazon EVS-Benutzerhandbuch beschreibt alle Amazon EVS-Konzepte und enthält Anweisungen zur Verwendung der verschiedenen Funktionen sowohl mit der Konsole als auch mit der Befehlszeilenschnittstelle.	9. Juni 2025

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.