Leitfaden

Amazon Elastic VMware Service

Amazon Elastic VMware Service: Leitfaden

Table of Contents

Was ist Amazon Elastic VMware Service?

> **Note**
>
> Amazon EVS befindet sich in der öffentlichen Vorschauversion und kann sich ändern.

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, `AWS::EVS::Environment` z. 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

> **Note**
>
> Amazon EVS befindet sich in der öffentlichen Vorschauversion und kann sich ändern.

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-Domäne mit einem vSphere-Cluster, der die Komponenten für die Verwaltung, 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 ESXi Host, der auf Amazon EC2 Bare-Metal-Instances ausgeführt wird.

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-Geräten und Hosts zu erleichtern. ESXi 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. Amazon EVS VLAN-Subnetze haben eine minimale CIDR-Blockgröße von /28 und eine maximale Größe von /24. 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. 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.

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

VMkernel VLAN-Subnetz für Hostverwaltung

Das VMkernel 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-Hosts zu kapseln und zu entkapseln. ESXi

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 Hosts verwendet. ESXi

VLAN-Subnetz für die VM-Verwaltung

Das VM-Management-VLAN-Subnetz 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 aktiver und 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

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 AWS Direct Connect mithilfe eines AWS Site-to-Site VPN-Anhangs zu einem Transit-Gateway konfigurieren. Weitere Informationen finden Sie unter Migration.

Amazon EVS-Architektur

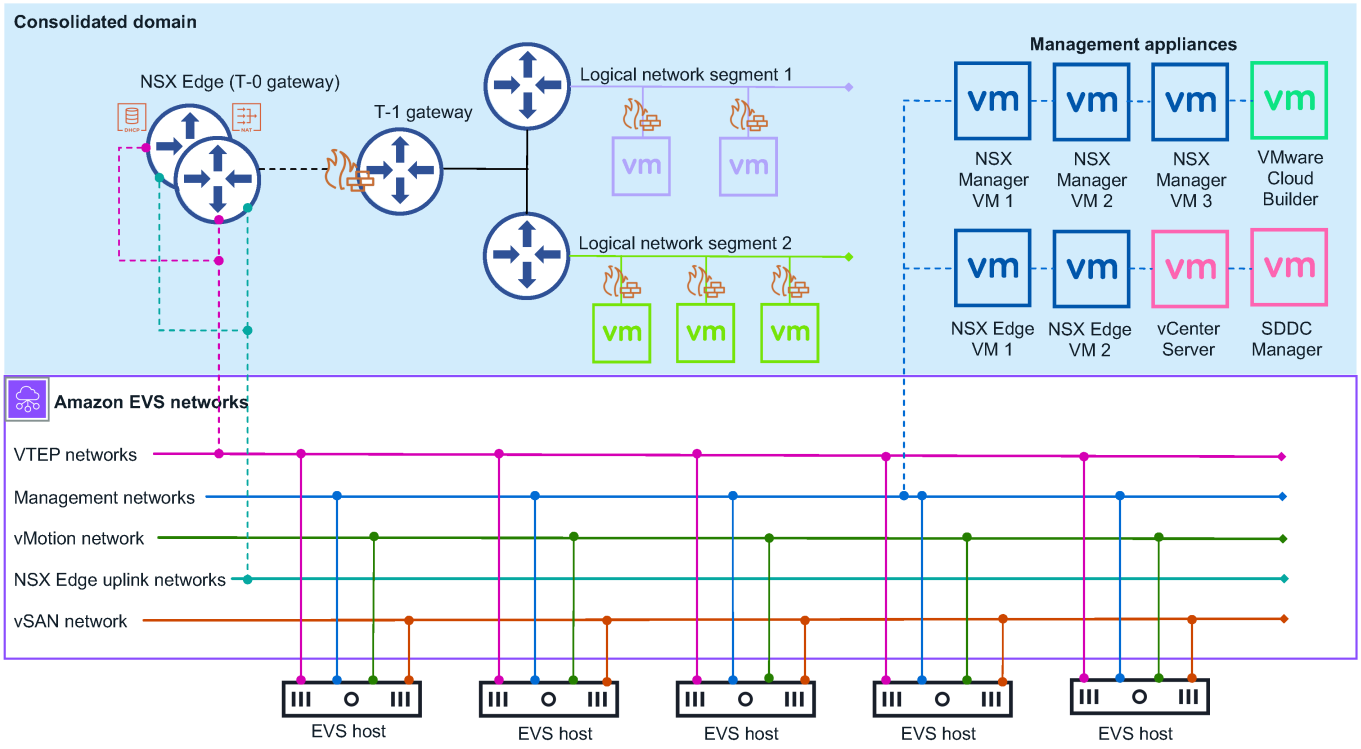
> **Note**
>
> Amazon EVS befindet sich in der öffentlichen Vorschauversion und kann sich ändern.

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:

- ESXi 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 Aktiv-/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 AWS 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 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-Konfiguration”.
- Amazon EVS VLAN-Subnetz-CIDR-Blöcke für jedes VLAN-Subnetz, das Amazon EVS bei der Umgebungserstellung für Sie bereitstellt. Amazon EVS VLAN-Subnetze haben eine minimale CIDR-Blockgröße von /28 und eine maximale Größe von /24. 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, als Peer nutzen.

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 Aktiv-/Standby-Modus ausgeführt werden. 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 Management Console 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 ESXi EVS-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

> **Note**
>
> Amazon EVS befindet sich in der öffentlichen Vorschauversion und kann sich ändern.

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.

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 EC2 Amazon-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 Sie VCF-Lizenzschlüssel
- VMware HCX-Voraussetzungen

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 bei der IAM-Konsole als Kontoinhaber an, indem Sie Root user (Stammbenutzer) 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. Markieren Sie das Kontrollkästchen neben AWS Management Console access (Zugriff auf AWS-Managementkonsole). Wählen Sie dann Custom password (Benutzerdefiniertes Passwort) aus und geben Sie danach ein neues Passwort in das Textfeld ein.
5. (Optional) Standardmäßig erfordert AWS, dass der neue Benutzer bei der ersten Anmeldung ein neues Passwort erstellt. 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 Filter policies (Richtlinien filtern) und anschließend AWS-managed job function (AWS-verwaltete Aufgabenfunktion) 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 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.

Mit diesen Schritten können Sie weitere Gruppen und Benutzer erstellen und Ihren Benutzern Zugriff auf Ihre AWS-Kontoressourcen gewähren. Informationen zur Verwendung von Richtlinien, die Benutzerberechtigungen auf bestimmte AWS-Ressourcen einschränken, finden Sie unter Zugriffsmanagement 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 Richtlinieneditor 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 Tags hinzu, um diese Ressource zu identifizieren, zu organisieren oder nach ihr zu suchen.
9. Wählen Sie Richtlinie erstellen aus.
10. Wählen Sie im linken Menü 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 Person als AWS-Konto 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 Zugriff auf den technischen Support und die Architekturberatung von Amazon EVS zu erhalten. 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 aktivieren, stellen Sie sicher, dass Ihr Konto den erforderlichen Mindestkontingentwert von 4 für die Hostanzahl pro EVS-Umgebungskontingent hat. Der Standardwert lautet 0. Weitere Informationen finden Sie unter the section called "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

Um die Erstellung einer Amazon EVS-Umgebung zu ermöglichen, müssen Sie Amazon EVS eine VPC zur Verfügung stellen, die ein Subnetz und ausreichend IP-Adressraum enthält, damit Amazon EVS die VLAN-Subnetze erstellen kann, die eine Verbindung zu Ihren VCF-Appliances herstellen. Weitere Informationen erhalten Sie unter the section called “Überlegungen zum Amazon EVS-Netzwerk” und the section called “Amazon EVS VLAN-Subnetz”.

Erstellen Sie eine EC2 Amazon-Kapazitätsreservierung

Amazon EVS startet Amazon EC2 i4i.metal-Instances, die ESXi Hosts in Ihrer Amazon EVS-Umgebung darstellen. Um sicherzustellen, dass Ihnen bei Bedarf ausreichend i4i.metal-Instance-Kapazität zur Verfügung steht, empfehlen wir Ihnen, eine EC2 Amazon-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 5.2.1 vertraut machen. Weitere Informationen finden Sie in den Versionshinweisen zu VCF 5.2.1

> **Note**
>
> Amazon EVS unterstützt derzeit nur VCF-Version 5.2.1.x.

Erwerben Sie VCF-Lizenzschlüssel

Um Amazon EVS verwenden zu können, müssen Sie einen VCF-Lösungsschlüssel und einen vSAN-Lizenzschlüssel angeben. Der VCF-Lösungsschlüssel muss mindestens 256 Kerne haben. Der vSAN-Lizenzschlüssel muss mindestens 110 TiB vSAN-Kapazität haben. Weitere Informationen zu VCF-Lizenzen finden Sie unter Verwaltung von Lizenzschlüsseln in VMware Cloud Foundation im Cloud Foundation-AdministrationshandbuchVMware .

> **Note**
>
> 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. Wenn Sie diese Schlüssel mit dem vSphere Client verwalten, müssen Sie sicherstellen, dass diese Schlüssel auch im Lizenzierungsbildschirm der SDDC Manager-Benutzeroberfläche angezeigt werden.

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.

- 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.
- VMware NSX ist in Ihrer Umgebung installiert und konfiguriert. Weitere Informationen finden Sie im VMware NSX-Installationshandbuch.
- VMware HCX ist in Ihrer Umgebung aktiviert und installiert. Weitere Informationen finden Sie unter „Erste Schritte mit VMware HCX“ im Handbuch Erste Schritte mit VMware HCX.

Erste Schritte mit Amazon Elastic VMware Service

> **Note**
>
> Amazon EVS befindet sich in der öffentlichen Vorschauversion und kann sich ändern.

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 5.2.1 vertraut machen. Weitere Informationen finden Sie in den Versionshinweisen zu VCF 5.2.1.

> **Important**
>
> Amazon EVS unterstützt derzeit nur VCF-Version 5.2.1.x.

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.

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. Amazon EVS-Subnetze haben

eine minimale CIDR-Blockgröße von /28 und eine maximale Größe von /24. 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 EC2 Bare-Metal-Instances in Ihrem Namen.
7. Wählen Sie für Anzahl der Availability Zones (AZs) die Option 1.

> **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 unterEndpunkte und Kontingente.

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.
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. VPC-Subnetze müssen eine minimale CIDR-Blockgröße von /28 haben. Amazon EVS VLAN-Subnetze haben eine minimale CIDR-Blockgröße von /28 und eine maximale Größe von /24.

12. (Optional) Um Internetzugriff auf Ressourcen IPv4 zu gewähren, wählen Sie für NAT-Gateways In 1 AZ. 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**
>
> Amazon VPC erstellt automatisch eine Haupt-Routing-Tabelle und ordnet dieser standardmäßig Subnetze zu. Amazon EVS erstellt Subnetze in der Haupt-Routing-Tabelle.

Konfigurieren Sie DNS- und NTP-Server mithilfe des VPC-DHCP-Optionssatzes

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

- DNS-Server (Domain Name System), die zur Auflösung von Host-IP-Adressen verwendet werden.

- NTP-Server (Network Time Protocol), die verwendet werden, um Probleme mit der Zeitsynchronisierung im SDDC zu vermeiden.

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

DNS-Server-Konfiguration

Sie können IPv4 Adressen von bis zu vier DNS-Servern (Domain Name System) eingeben. Sie können es Route 53 als Ihren DNS-Serveranbieter verwenden oder Ihre eigenen benutzerdefinierten DNS-Server bereitstellen. Weitere Informationen zur Konfiguration von Route 53 als DNS-Dienst für eine bestehende Domäne finden Sie unter Route 53 zum DNS-Dienst für eine verwendete Domäne machen.

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

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

Um eine 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, wie unter beschrieben. the section called “Erstellen Sie eine Amazon EVS-Umgebung”
- Eine Reverse-Lookupzone mit PTR-Datensätzen für jede VCF-Verwaltungs-Appliance und jeden Amazon EVS-Host in Ihrer Bereitstellung, wie unter beschrieben. the section called “Erstellen Sie eine Amazon EVS-Umgebung”

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

> **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.

NTP-Serverkonfiguration

NTP-Server stellen die Zeit in Ihrem Netzwerk bereit. Sie können die IPv4 Adressen von bis zu vier NTP-Servern (Network Time Protocol) eingeben. Weitere Informationen zur Konfiguration von NTP-Servern in einem DHCP-Optionssatz finden Sie unter Erstellen eines DHCP-Optionssatzes.

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

Sie können den Amazon Time Sync Service unter der IPv4 Adresse angeben`169.254.169.123`. Standardmäßig verwenden die EC2 Amazon-Instances, die Amazon EVS bereitstellt, den Amazon Time Sync Service an IPv4 der Adresse. `169.254.169.123`

Weitere Informationen zu NTP-Servern finden Sie unter RFC 2123. Weitere Informationen zum Amazon Time Sync Service finden Sie unter Zeit für Ihre Instance festlegen im EC2 Amazon-Benutzerhandbuch.

(Optional) Konfigurieren Sie die lokale Netzwerkkonnektivität mithilfe von AWS Direct Connect oder AWS Site-to-Site VPN mit AWS Transit Gateway

Sie können die Konnektivität Ihres lokalen Rechenzentrums AWS Direct Connect mit Ihrer AWS Infrastruktur mithilfe eines zugehörigen Transit-Gateways oder mithilfe einer AWS Site-to-Site

VPN-Verbindung zu einem Transit-Gateway konfigurieren. AWS Site-to-Site VPN stellt über das Internet eine IPsec VPN-Verbindung zum Transit-Gateway her. AWS Direct Connect stellt über eine private, dedizierte Verbindung eine IPsec VPN-Verbindung zum Transit-Gateway her. Nachdem die Amazon EVS-Umgebung erstellt wurde, können Sie beide Optionen verwenden, um Ihre lokalen Rechenzentrums-Firewalls mit der VMware NSX-Umgebung zu verbinden.

> **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.

Weitere Informationen zum Einrichten einer AWS Direct Connect Verbindung finden Sie unter AWS 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.

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 konfigurierte Peer-ASN muss übereinstimmen und die Peer-IP-Adressen müssen eindeutig sein.

> **Important**
>
> Wenn Sie die Route-Server-Propagierung aktivieren, stellen Sie 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.

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

> **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.

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**
>
> 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.

   > **Note**
   >
   > Amazon EVS-Operationen, die von der Amazon EVS-Konsole ausgelöst werden, generieren CloudTrail keine Ereignisse.

2. Wählen Sie im Navigationsbereich Environments (Umgebungen) aus.
3. Wählen Sie Create environment (Umgebung erstellen) aus.
4. Gehen Sie auf der Seite „Amazon EVS-Anforderungen validieren“ wie folgt vor.
   a. Vergewissern Sie sich, dass die AWS Support-Anforderungen und die Service-Quota-Anforderungen erfüllt sind. Weitere Informationen zu den Support-Anforderungen von Amazon EVS finden Sie unterthe section called “Melden Sie sich für einen AWS Business-,

AWS Enterprise On-Ramp- oder AWS Enterprise Support-Plan an". Weitere Informationen zu den Amazon EVS-Kontingentanforderungen finden Sie unterthe section called "Servicekontingente".

b. (Optional) Geben Sie unter Name einen Umgebungsnamen ein.

c. Wählen Sie unter Umgebungsversion Ihre VCF-Version aus. Amazon EVS unterstützt derzeit nur Version 5.2.1.x.

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

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

> **Note**
>
> Der VCF-Lösungsschlüssel muss mindestens 256 Kerne haben.

> **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.

f. 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 mindestens 110 TiB vSAN-Kapazität haben.

> **Note**
>
> Amazon EVS erfordert, dass Sie einen gültigen vSAN-Lizenzschlüssel im SDDC Manager verwalten, damit der Service 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.

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

h. Wählen Sie Weiter aus.

5. Führen Sie auf der Seite „Hostdetails angeben“ die folgenden Schritte viermal durch, um der Umgebung 4 Hosts hinzuzufügen. Amazon EVS-Umgebungen benötigen 4 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 zum Beispiel Instanztyp den EC2 Instanztyp aus.

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

> **Note**
>
> Amazon EVS unterstützt derzeit nur EC2 i4i.metal-Instances.

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

   e. Wählen Sie Host hinzufügen.

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

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

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

   c. Für Sicherheitsgruppe — optional können Sie bis zu 2 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.

d. Geben Sie unter Management-Konnektivität die CIDR-Blöcke ein, die für die Amazon EVS-VLAN-Subnetze verwendet werden sollen.

> **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”.

e. 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.

> **Note**
>
> Stellen Sie sicher, dass die von Ihnen bereitgestellten VLAN-CIDR-Blöcke innerhalb der VPC die richtige Größe haben. Weitere Informationen finden Sie unter the section called “Überlegungen zum Amazon EVS-Netzwerk”.

f. Geben Sie unter Workload/VCF-Konnektivität den CIDR-Block für das NSX-Uplink-VLAN ein und wählen Sie 2 VPC-Route-Server-Peer aus, IDs die über den NSX-Uplink zu Route Server-Endpunkten führen.

> **Note**
>
> Amazon EVS benötigt eine VPC-Route-Server-Instance, die mit 2 Route Server-Endpunkten und 2 Route Server-Peers verknüpft 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”.

g. 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 mit der Amazon EVS-Umgebung verknüpft 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.

> **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 zu den Support-Anforderungen von Amazon EVS finden Sie unterthe section called “Melden Sie sich für einen AWS Business-, AWS Enterprise On-Ramp- oder AWS Enterprise Support-Plan an”. Weitere Informationen zu den Amazon EVS-Kontingentanforderungen finden Sie unterthe section called “Servicekontingente”.

> **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 Erstellung 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.
- Denn `--vcf-version` Amazon EVS unterstützt derzeit nur VCF 5.2.1.x.
- 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 über Ihre VCF-Software in Amazon EVS werden an Broadcom weitergegeben, um die Einhaltung der Lizenzbestimmungen zu überprüfen.
- Geben Sie für `--license-info` Ihren VCF-Lösungsschlüssel und Ihren vSAN-Lizenzschlüssel ein.

> **Note**
>
> Der VCF-Lösungsschlüssel muss mindestens 256 Kerne haben. Der vSAN-Lizenzschlüssel muss mindestens 110 TiB vSAN-Kapazität haben.

> **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.

> **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 Instanztyp an.

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

  > **Note**
  >
  > Amazon EVS unterstützt derzeit nur EC2 i4i.metal-Instances.

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

  > **Note**
  >
  > Amazon EVS benötigt eine VPC-Route-Server-Instance, die mit 2 Route Server-Endpunkten und 2 Route Server-Peers verknüpft 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 Ihres Softwarevertrags oder Ihrer Vertragsverlängerung zur Verfügung gestellt.
- (Optional) Geben Sie für die Region ein`--region`, 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-5.2.1 \
```

```
--terms-accepted \
--license-info "{
      \"solutionKey\": \"00000-00000-00000-abcde-11111\",
      \"vsanKey\": \"00000-00000-00000-abcde-22222\"
    }" \
   --initial-vlans "{
      \"vmkManagement\": {
        \"cidr\": \"10.10.0.0/24\"
      },
      \"vmManagement\": {
        \"cidr\": \"10.10.1.0/24\"
      },
      \"vMotion\": {
        \"cidr\": \"10.10.2.0/24\"
      },
      \"vSan\": {
        \"cidr\": \"10.10.3.0/24\"
      },
      \"vTep\": {
        \"cidr\": \"10.10.4.0/24\"
      },
      \"edgeVTep\": {
        \"cidr\": \"10.10.5.0/24\"
      },
      \"nsxUplink\": {
        \"cidr\": \"10.10.6.0/24\"
      },
      \"hcx\": {
        \"cidr\": \"10.10.7.0/24\"
      },
      \"expansionVlan1\": {
        \"cidr\": \"10.10.8.0/24\"
      },
      \"expansionVlan2\": {
          \"cidr\": \"10.10.9.0/24\"
      }
    }" \
--hosts "[
    {
      \"hostName\": \"esx01\",
      \"keyName\": \"sshKey-04-05-45\”,
      \"instanceType\": \"i4i.metal\"
    },
    {
```

```
      \"hostName\": \"esx02\",
      \"keyName\": \"sshKey-04-05-45\",
      \"instanceType\": \"i4i.metal\"
    },
    {
      \"hostName\": \"esx03\",
      \"keyName\": \"sshKey-04-05-45\",
      \"instanceType\": \"i4i.metal\"
    },
    {
      \"hostName\": \"esx04\",
      \"keyName\": \"sshKey-04-05-45\",
      \"instanceType\": \"i4i.metal\"
    }
  ]" \
--connectivity-info "{
    \"privateRouteServerPeerings\": [\"rsp-1234567890abcdef0\",\"rsp-
abcdef01234567890\"]
  }" \
  --vcf-hostnames "{
    \"vCenter\": \"vcf-vc01\",
    \"nsx\": \"vcf-nsx\",
    \"nsxManager1\": \"vcf-nsxm01\",
    \"nsxManager2\": \"vcf-nsxm02\",
    \"nsxManager3\": \"vcf-nsxm03\",
    \"nsxEdge1\": \"vcf-edge01\",
    \"nsxEdge2\": \"vcf-edge02\",
    \"sddcManager\": \"vcf-sddcm01\",
    \"cloudBuilder\": \"vcf-cb01\"
  }" \
--site-id my-site-id \
--region us-east-2
```

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-5.2.1",
        "termsAccepted": true,
        "licenseInfo": [
            {
                "solutionKey": "00000-00000-00000-abcde-11111",
                "vsanKey": "00000-00000-00000-abcde-22222"
            }
        ],
        "siteId": "my-site-id",
        "connectivityInfo": {
            "privateRouteServerPeerings": [
                "rsp-1234567890abcdef0",
                "rsp-abcdef01234567890"
            ]
        },
        "vcfHostnames": {
            "vCenter": "vcf-vc01",
            "nsx": "vcf-nsx",
            "nsxManager1": "vcf-nsxm01",
            "nsxManager2": "vcf-nsxm02",
            "nsxManager3": "vcf-nsxm03",
            "nsxEdge1": "vcf-edge01",
            "nsxEdge2": "vcf-edge02",
            "sddcManager": "vcf-sddcm01",
            "cloudBuilder": "vcf-cb01"
        }
    }
}
```

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-5.2.1",
        "termsAccepted": true,
        "licenseInfo": [
            {
                "solutionKey": "00000-00000-00000-abcde-11111",
                "vsanKey": "00000-00000-00000-abcde-22222"
            }
        ],
        "siteId": "my-site-id",
        "checks": [],
        "connectivityInfo": {
            "privateRouteServerPeerings": [
                "rsp-056b2b1727a51e956",
                "rsp-07f636c5150f171c3"
            ]
        },
        "vcfHostnames": {
            "vCenter": "vcf-vc01",
            "nsx": "vcf-nsx",
            "nsxManager1": "vcf-nsxm01",
            "nsxManager2": "vcf-nsxm02",
            "nsxManager3": "vcf-nsxm03",
            "nsxEdge1": "vcf-edge01",
            "nsxEdge2": "vcf-edge02",
            "sddcManager": "vcf-sddcm01",
            "cloudBuilder": "vcf-cb01"
        },
        "credentials": []
    }
}
```

Amazon EVS VLAN-Subnetze einer Routing-Tabelle zuordnen

Ordnen Sie jedes der Amazon EVS-VLAN-Subnetze 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.

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
```

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.

> **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.

Rufen Sie VCF-Anmeldeinformationen ab und greifen Sie auf VCF-Verwaltungs-Appliances 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. Weitere Informationen zum Abrufen von Geheimnissen finden Sie unter Geheimnisse aus AWS Secrets Manager abrufen.

> **Note**
>
> Amazon EVS bietet keine verwaltete Rotation Ihrer Geheimnisse. Wir empfehlen, dass Sie Ihre Geheimnisse regelmäßig innerhalb eines festgelegten Rotationsfensters rotieren, um sicherzustellen, dass die Geheimnisse nicht langlebig sind.

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 Konsole EC2

Standardmäßig aktiviert Amazon EVS die ESXi Shell auf neu bereitgestellten Amazon EVS-Hosts. Diese Konfiguration ermöglicht den Zugriff auf die serielle Schnittstelle der EC2 Amazon-Instance über die EC2 serielle 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 EC2 serielle Konsole kann über die EC2 Konsole oder die zugegriffen werden AWS CLI. Weitere Informationen finden Sie unter EC2 Serial Console for Instances im EC2 Amazon-Benutzerhandbuch.

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

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

Connect zur EC2 seriellen Konsole her

Um eine Verbindung zur EC2 seriellen 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 EC2 serielle Konsole und Connect zur EC2 seriellen Konsole herstellen im EC2 Amazon-Benutzerhandbuch.

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

Konfigurieren Sie den Zugriff auf die EC2 serielle Konsole

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

SDDC UI and Amazon EVS console

1. Gehen Sie zur SDDC Manager-Benutzeroberfläche.
2. Entfernen Sie die Hosts aus dem vSphere-Cluster. Dadurch wird die Zuweisung der Hosts zur SDDC-Domäne aufgehoben. Wiederholen Sie diesen Schritt für jeden Host im Cluster. Weitere Informationen finden Sie unter Entfernen eines Hosts aus einem vSphere-Cluster in einer Workload-Domäne in der VCF-Produktdokumentation.
3. Nehmen Sie die nicht zugewiesenen Hosts außer Betrieb. Weitere Informationen finden Sie in der VCF-Produktdokumentation unter Außerbetriebnahme von Hosts.
4. Gehen Sie zur Amazon EVS-Konsole.

> **Note**
>
> Amazon EVS-Operationen, die von der Amazon EVS-Konsole ausgelöst werden, generieren CloudTrail keine Ereignisse.

5. Wählen Sie im Navigationsbereich Umgebung aus.
6. Wählen Sie die Umgebung aus, die die zu löschenden Hosts enthält.
7. Wählen Sie die Registerkarte Hosts aus.
8. Wählen Sie den Host aus und klicken Sie auf der Registerkarte „Hosts“ auf Löschen. Wiederholen Sie diesen Schritt für jeden Host in der Umgebung.
9. 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.

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

SDDC UI and 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-5.2.1",
            "environmentState": "CREATED",
            "createdAt": "2025-04-13T14:42:41.430000+00:00",
            "modifiedAt": "2025-04-13T14:43:33.412000+00:00",
            "environmentArn": "arn:aws:evs:us-east-2:111122223333:environment/env-
abcde12345"
        },
        {
            "environmentId": "env-edcba54321",
            "environmentName": "testEnv2",
            "vcfVersion": "VCF-5.2.1",
            "environmentState": "CREATED",
            "createdAt": "2025-04-13T13:39:49.546000+00:00",
            "modifiedAt": "2025-04-13T13:52:13.342000+00:00",
            "environmentArn": "arn:aws:evs:us-east-2:111122223333:environment/env-
edcba54321"
        }
    ]
}
```

3. Gehen Sie zur SDDC Manager-Benutzeroberfläche.
4. Entfernen Sie die Hosts aus dem vSphere-Cluster. Dadurch wird die Zuweisung der Hosts zur SDDC-Domäne aufgehoben. Wiederholen Sie diesen Schritt für jeden Host im Cluster. Weitere Informationen finden Sie unter Entfernen eines Hosts aus einem vSphere-Cluster in einer Workload-Domäne in der VCF-Produktdokumentation.
5. Nehmen Sie die nicht zugewiesenen Hosts außer Betrieb. Weitere Informationen finden Sie in der VCF-Produktdokumentation unter Außerbetriebnahme von Hosts.
6. 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
```

7. Wiederholen Sie die vorherigen Schritte, um die verbleibenden Hosts in Ihrer Umgebung zu löschen.
8. 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.

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

Löschen Sie die VPC-Route-Server-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.

Löschen Sie elastische Netzwerkschnittstellen

Schritte zum Löschen elastischer Netzwerkschnittstellen finden Sie unter Löschen einer Netzwerkschnittstelle im EC2 Amazon-Benutzerhandbuch.

Trennen und löschen Sie Subnetz-Routing-Tabellen

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 VMware Hybrid Cloud Extension (VMware HCX) zu Amazon EVS

> **Note**
>
> Amazon EVS befindet sich in der öffentlichen Vorschauversion und kann sich ändern.

Nachdem Sie eine Amazon EVS-Umgebung erstellt haben, können Sie Ihre vorhandenen VMware basierten Workloads mithilfe der VMware Hybrid Cloud Extension (HCX) zu Amazon Elastic VMware Service (Amazon EVS) migrieren. VMware Weitere Informationen zur VMware HCX-Migration finden Sie unter HCX-Migrationstypen im VMware HCX-Benutzerhandbuch. VMware

Das folgende Tutorial beschreibt, wie Sie VMware HCX verwenden, um einen VMware Workload zu Amazon EVS zu migrieren.

Sie können VMware HCX verwenden, um Workloads über eine private Verbindung mithilfe eines zugehörigen Transit-Gateways oder AWS Direct Connect mithilfe eines AWS Site-to-Site VPN-Anhangs zu einem Transit-Gateway zu migrieren.

> **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.

Weitere Informationen zum Einrichten einer AWS Direct Connect Verbindung finden Sie unter AWS Direct Connect Gateways und Transit-Gateway-Verknüpfungen im Benutzerhandbuch. AWS Direct Connect 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.

Voraussetzungen

Bevor Sie VMware HCX mit Amazon EVS verwenden, stellen Sie sicher, dass die HCX-Voraussetzungen erfüllt sind und dass eine Amazon EVS-Umgebung erstellt und mit Ihrem lokalen

Netzwerk verbunden wurde, entweder AWS Direct Connect mit einem Transit-Gateway oder einem AWS Site-to-Site VPN mit einem Transit-Gateway. Schritte zum Erstellen einer Amazon EVS-Umgebung finden Sie unterErste Schritte. Weitere Informationen zu den VMware HCX-Voraussetzungen finden Sie unter. the section called “VMware HCX-Voraussetzungen”

Überprüfen Sie den Status des HCX-VLAN-Subnetzes

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 VLANsunter das HCX-VLAN und überprüfen Sie, ob der Status Created lautet.
6. Kopieren Sie die `vlan` HCX-ID für die spätere Verwendung.

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
```

Im Folgenden wird eine Beispielantwort dargestellt:

```
{
 "environmentVlans": [
        {
            "vlan": 80,
            "cidr": "10.10.7.0/24",
```

```
            "availabilityZone": "us-east-2c",
            "functionName": "hcx",
            "createdAt": "2025-04-13T13:39:58.845000+00:00",
            "modifiedAt": "2025-04-13T13:47:57.067000+00:00",
            "vlanState": "CREATED",
            "stateDetails": ""
        },
        {
            "vlan": 20,
            "cidr": "10.10.1.0/24",
            "availabilityZone": "us-east-2c",
            "functionName": "vmManagement",
            "createdAt": "2025-04-13T13:39:58.456000+00:00",
            "modifiedAt": "2025-04-13T13:47:57.524000+00:00",
            "vlanState": "CREATED",
            "stateDetails": ""
        }
 ]
}
```


2. Identifizieren Sie das VLAN mit einem `functionName` von `hcx` und überprüfen Sie, ob das `vlanState` ist`CREATED`.
3. Kopieren Sie die `vlan` HCX-ID zur späteren Verwendung.

Stellen Sie sicher, 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”

Example

Amazon VPC console

1. Gehen Sie zur Amazon VPC Konsole.
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.

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

Der HCX WAN Optimization Service (HCX-WAN-OPT) 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-WAN-IX) bereitgestellt. HCX-WAN-IX ist verantwortlich für die Datenreplikation zwischen der Unternehmensumgebung und der Amazon EVS-Umgebung.

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 des Workload-Datenverkehrs zu Amazon EVS zu konfigurieren und so einen langen Round-Trip-Netzwerkpfad durch das Quell-Gateway zu vermeiden. 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 Einschränkungen 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.

Sicherheit in Amazon Elastic VMware Service

> **Note**
>
> Amazon EVS befindet sich in der öffentlichen Vorschauversion und kann sich ändern.

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 gelten, finden Sie unter AWS-Services 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.

In dieser Dokumentation erfahren Sie, wie Sie das Modell der gemeinsamen Verantwortung bei der Nutzung von Amazon Elastic VMware Service anwenden können. Es zeigt Ihnen, wie Sie Amazon Elastic VMware Service konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere verwenden können AWS-Services , die Ihnen helfen, Ihre Amazon Elastic VMware Service-Ressourcen zu überwachen und zu sichern.

Inhalt

Identitäts- und Zugriffsmanagement für Amazon Elastic VMware Service

> **Note**
>
> Amazon EVS befindet sich in der öffentlichen Vorschauversion und kann sich ändern.

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-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 Elastic VMware Service ausführen.

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

Service-Administrator — Wenn Sie in Ihrem Unternehmen für die Amazon Elastic VMware Service-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf Amazon Elastic VMware Service. Es ist Ihre Aufgabe, zu bestimmen, auf welche Funktionen und Ressourcen von Amazon Elastic VMware Service 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 Elastic VMware Service nutzen IAM kann, finden Sie unterthe section called “So funktioniert Amazon Elastic VMware Service 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 Elastic VMware Service zu verwalten. Beispiele für identitätsbasierte Richtlinien von Amazon Elastic VMware Service, die Sie verwenden können IAM, finden Sie unter Beispiele für identitätsbasierte Richtlinien von Amazon Elastic VMware Service.

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, an oder IAM-Benutzer, 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 Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung bei 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 Signaturprozess für Signature Version 4 in der Allgemeinen AWS-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.

Root-Benutzer des AWS-Kontos

Wenn Sie zum ersten Mal eine erstellen AWS-Konto, beginnen Sie mit einer Single-Sign-In-Identität, die vollständigen Zugriff auf alle Ressourcen im Konto hat. AWS-Services Diese Identität wird als AWS-Konto-Stammbenutzer bezeichnet. Um auf den Stammbenutzer zuzugreifen, müssen Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, die zur Erstellung des Kontos verwendet wurden. 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 vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise einer Gruppe einen Namen geben IAMAdminsund dieser Gruppe Berechtigungen zur Verwaltung von IAM Ressourcen erteilen.

Benutzer unterscheiden sich von 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 Management Console 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 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 Management Console 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. Inline-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. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- 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. SCPs schränken Berechtigungen für Entitäten in Mitgliedskonten einschließlich des jeweiligen Root-Benutzer des AWS-Kontos ein. Weitere Informationen zu Organisationen 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 mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter Bewertungslogik für Richtlinien.

So funktioniert Amazon Elastic VMware Service mit IAM

> **Note**
>
> Amazon EVS befindet sich in der öffentlichen Vorschauversion und kann sich ändern.

Bevor Sie IAM den Zugriff auf Amazon Elastic VMware Service verwalten, sollten Sie sich darüber informieren, welche IAM Funktionen für Amazon Elastic VMware Service 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 Elastic VMware Service und andere AWS-Services Unternehmen AWS-Services damit arbeiten IAM, finden Sie IAM im IAM-Benutzerhandbuch.

Themen

- Identitätsbasierte Richtlinien für Amazon EVS
- Zugriffskontrolllisten (ACLs) in Amazon EVS
- Attributbasierte Zugriffskontrolle (ABAC) mit Amazon EVS
- Temporäre Anmeldeinformationen mit Amazon EVS verwenden
- Zugriffssitzungen für Amazon EVS weiterleiten
- Servicerollen für Amazon EVS
- Servicebezogene Rollen für Amazon EVS

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 Richtlinien von Amazon Elastic VMware Service finden Sie unter Beispiele für identitätsbasierte Richtlinien von Amazon Elastic VMware Service.

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 festlegen, wer zum Zugriff auf was berechtigt ist. 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 Elastic VMware Service 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 Elastic VMware Service 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 Elastic VMware Service-Aktionen finden Sie unter Von Amazon Elastic VMware Service definierte Aktionen in der Service Authorization Reference.

Richtlinienressourcen für Amazon EVS

Unterstützt politische Ressourcen: Teilweise

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. 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 bei Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, wie z. B. das Auflisten von Vorgängen, 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 festlegen, wer zum Zugriff auf was berechtigt ist. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Mit dem `Condition` Element (oder `Condition` Block) können Sie 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 auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. 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 Elastic VMware Service definiert seinen eigenen Satz von Bedingungsschlüsseln und unterstützt auch die Verwendung einiger globaler Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel 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 Elastic VMware Service-Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für Amazon Elastic VMware Service in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von Amazon Elastic VMware Service 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 Elastic VMware Service-Ressourcen anhängen oder Tags in einer Anfrage an Amazon Elastic VMware Service 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 Management Console 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-Anfragen 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 Elastic VMware Service-Rollen finden Sie unterthe section called “Verwenden von serviceverknüpften Rollen”.

Beispiele für identitätsbasierte Amazon EVS-Richtlinien

> **Note**
>
> Amazon EVS befindet sich in der öffentlichen Vorschauversion und kann sich ändern.

Standardmäßig sind Rollen nicht berechtigt, IAM-Benutzer Amazon Elastic VMware Service-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mit der AWS Management Console 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

- Bewährte Methoden für Richtlinien
- Verwenden der Amazon Elastic VMware Service-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

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand Amazon Elastic VMware Service-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Erste Schritte mit AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten — Um Ihren Benutzern und Workloads zunächst Berechtigungen zu

gewähren, verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle 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 AWS -verwaltete Richtlinien oder AWS -verwaltete Richtlinien für Auftrags-Funktionen 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, wie AWS CloudFormation z. 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 Elastic VMware Service-Konsole

Um auf die Amazon Elastic VMware Service-Konsole zugreifen zu können, muss ein IAM-Principal über ein Mindestmaß an Berechtigungen verfügen. Diese Berechtigungen müssen es dem Principal ermöglichen, Details zu den Amazon Elastic VMware Service-Ressourcen in Ihrem aufzulisten und anzuzeigen AWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die restriktiver ist als die erforderlichen Mindestberechtigungen, funktioniert die Konsole für Prinzipale, denen diese Richtlinie zugewiesen ist, nicht wie vorgesehen.

Um sicherzustellen, dass Ihre IAM-Prinzipale weiterhin die Amazon Elastic VMware Service-Konsole 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 Erlauben Sie stattdessen nur den Zugriff auf die Aktionen, die dem API-Vorgang entsprechen, den 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"
            ],
            "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 Identität und Zugriff auf Amazon Elastic VMware Service

> **Note**
>
> Amazon EVS befindet sich in der öffentlichen Vorschauversion und kann sich ändern.

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit Amazon Elastic VMware Service und auftreten können IAM.

Themen

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 Elastic VMware Service-Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Bei Services, 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 Elastic VMware Service diese Funktionen unterstützt, finden Sie unterthe section called “So funktioniert Amazon Elastic VMware Service 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 Zugriff auf eine andere Ressource gewähren 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

> **Note**
>
> Amazon EVS befindet sich in der öffentlichen Vorschauversion und kann sich ändern.

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet AWS wird. AWS Verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele gängige Anwendungsfälle bereitstellen, 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 für alle AWS Kunden verfügbar sind. 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 keine Verbindungen `AmazonEVSServiceRolePolicy` zu Ihren IAM-Entitäten herstellen. 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 serviceverknüpften 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 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`- Erstellen, ändern, kennzeichnen und löschen Sie eine elastic network interface, die verwendet wird, um eine dauerhafte Verbindung zwischen Amazon EVS und einer SDDC Manager-Appliance der VMware Virtual Cloud Foundation (VCF) im VPC-Subnetz des Kunden herzustellen. Diese Konnektivität ist erforderlich, damit Amazon EVS die VCF-Bereitstellung bereitstellen, verwalten und überwachen kann.

Die neueste Version des JSON-Richtliniendokuments finden Sie bei 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.

Änderung	Beschreibung	Datum
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

> **Note**
>
> Amazon EVS befindet sich in der öffentlichen Vorschauversion und kann sich ändern.

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` Die Rolle ermöglicht Amazon EVS, Cluster in Ihrem Konto zu verwalten. Die beigefügten Richtlinien ermöglichen es der Rolle, die folgenden Ressourcen zu verwalten: Netzwerkschnittstellen, Sicherheitsgruppen, Protokolle und VPCs.

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 einen Cluster in der AWS Management Console, 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 es 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 Endpunkte und Kontingente.

Amazon EVS mit anderen AWS Diensten verwenden

> **Note**
>
> Amazon EVS befindet sich in der öffentlichen Vorschauversion und kann sich ändern.

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

> **Note**
>
> Amazon EVS befindet sich in der öffentlichen Vorschauversion und kann sich ändern.

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 die ersten Schritte mit Vorlagen zu erleichtern. 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

> **Note**
>
> Amazon EVS befindet sich in der öffentlichen Vorschauversion und kann sich ändern.

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 virtuelle Maschinen, die auf Amazon EVS laufen. VMware

FSx Für NetApp ONTAP als NFS-Datenspeicher konfigurieren

> **Note**
>
> Amazon EVS befindet sich in der öffentlichen Vorschauversion und kann sich ändern.

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 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.

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 for Single-AZ 1 or at least 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

> **Note**
>
> Amazon EVS befindet sich in der öffentlichen Vorschauversion und kann sich ändern.

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 for Single-AZ 1 or at least 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 Hostspeicher ESXi

Für jeden ESXi Host müssen Sie den Software-iSCSI-Adapter so konfigurieren, dass Ihre ESXi Hosts ihn für den Zugriff auf iSCSI-Speicher verwenden können. Anweisungen zur Konfiguration des Software-iSCSI-Adapters für ESXi 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 ESXi 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` existiert.

   ```
   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 ESXi 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 ESXi 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

> **Note**
>
> Amazon EVS befindet sich in der öffentlichen Vorschauversion und kann sich ändern.

In diesem Kapitel werden einige häufig auftretende Probleme bei der Erstellung oder Verwaltung von Amazon EVS-Umgebungen beschrieben.

Beheben Sie fehlgeschlagene Statusprüfungen der Umgebung

Amazon EVS führt automatisierte Prüfungen Ihrer Umgebung durch, um Probleme zu identifizieren. Sie können den Status Ihrer Umgebung einsehen, 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.

Wenn diese Prüfung fehlschlägt, kann Amazon EVS den SDDC Manager nicht mehr erreichen, um den Umgebungsstatus zu überprüfen, und es können keine Hosts mehr zur Umgebung hinzugefügt werden. Ein Fehler bei der Erreichbarkeit führt auch dazu, dass die Überprüfung der

Wiederverwendung von Lizenzschlüsseln und der Schlüsselabdeckung fehlschlägt und bei der Überprüfung der Host-Anzahl die Antwort Unbekannt zurückgegeben wird.

Erreichbarkeitsfehler deuten darauf hin, dass möglicherweise ein Problem mit dem SDDC Manager, der Firewallkonfiguration oder einem fehlenden Zertifikat vorliegt. Sie können versuchen, diese Probleme zu lösen, oder sich an den AWS Support wenden, um weitere 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 5.2.1.

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 der Umgebung eine gebrauchte Lizenz hinzugefügt wird.

Wenn diese Prüfung fehlschlägt, erhalten Sie eine Fehlermeldung, dass die Amazon EVS-Umgebung nicht erstellt werden konnte. Um das Problem zu beheben, überprüfen Sie Ihre Lizenzeinstellungen im SDDC Manager und ersetzen Sie alle zuvor verwendeten Lizenzen durch ungenutzte Lizenzen.

> **Important**
>
> Verwenden Sie die SDDC Manager-Benutzeroberfläche, um die Lizenzschlüssel für VCF-Komponenten zu verwalten. Amazon EVS erfordert, dass Sie gültige Komponentenlizenzschlüssel im SDDC Manager verwalten, damit der Service ordnungsgemäß funktioniert. Wenn Sie Komponentenlizenzschlüssel mit dem vSphere Client verwalten, müssen Sie sicherstellen, dass diese Schlüssel auch im Lizenzierungsbildschirm der SDDC Manager-Benutzeroberfläche angezeigt werden, um zu verhindern, dass die Lizenzschlüsselprüfung fehlschlägt.

Die Überprüfung der Schlüsselabdeckung ist fehlgeschlagen

Diese Prüfung stellt sicher, dass Ihr vCenter Server zugewiesener VCF-Lizenzschlüssel allen bereitgestellten Hosts ausreichend vCPU-Kerne und vSAN-Speicherkapazität (TiB) zuweist.

Wenn diese Prüfung fehlschlägt, erhalten Sie eine Fehlermeldung, dass die Amazon EVS-Umgebung nicht erstellt werden konnte oder der Umgebung kein Amazon EVS-Host hinzugefügt werden konnte. Ein Ausfall der Schlüsselabdeckung kann auf eines der folgenden Probleme hinweisen:

- Sie haben die Anzahl der unterstützten Hosts für Amazon EVS überschritten. Amazon EVS unterstützt 4 bis 16 Hosts pro Umgebung. Wenn dies das Problem ist, entfernen Sie Hosts oder fügen Sie sie hinzu, bis sich Ihre Umgebung im unterstützten Hostbereich befindet.
- VCF-Lizenzen sind vCenter Server nicht ordnungsgemäß zugewiesen. Sie müssen vCenter Server eine Lizenz zuweisen, bevor der Testzeitraum abläuft oder die aktuell zugewiesene Lizenz abläuft. Wenn dies das Problem ist, überprüfen Sie die Lizenzzuweisungen im SDDC Manager.
- Aktuelle VCF-Lizenzen decken den Bedarf an vCPU-Kern und vSAN-Speicherkapazität nicht ab. Der VCF-Lösungsschlüssel muss mindestens 256 Kerne haben. Der vSAN-Lizenzschlüssel muss über eine vSAN-Kapazität von mindestens 110 TiB verfügen. Wenn dies das Problem ist, fügen Sie vSAN-Lizenzen im SDDC Manager hinzu, bis Ihre Nutzungsanforderungen erfüllt sind.

Wenn das Problem durch die 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 Lizenzschlüssel für VCF-Komponenten zu verwalten. Amazon EVS erfordert, dass Sie gültige Komponentenlizenzschlüssel im SDDC Manager verwalten, damit der Service ordnungsgemäß funktioniert. Wenn Sie Komponentenlizenzschlüssel mit dem vSphere Client verwalten, müssen Sie sicherstellen, dass diese Schlüssel auch im Lizenzierungsbildschirm der SDDC Manager-Benutzeroberfläche angezeigt werden, um zu verhindern, dass die Lizenzschlüsselprüfung fehlschlägt.

Der vSphere HA-Agent auf diesem Host konnte die Isolationsadresse nicht erreichen

Auf der vCenter-Benutzeroberfläche wird bei ausgewähltem ESXi Host die Meldung „Der vSphere HA-Agent auf diesem Host konnte die Isolationsadresse < IPv6 Adresse> 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.

Um die vSphere HA-Fehlermeldung zu entfernen, müssen Sie vSphere HA deaktivieren. Schritte zur Deaktivierung von vSphere HA im vSphere-Client finden Sie im Broadcom-Artikel Disabling and enabling VMware High Availability (HA).

Amazon Elastic VMware Service-Endpunkte und Kontingente

> **Note**
>
> Amazon EVS befindet sich in der öffentlichen Vorschauversion und kann sich ändern.

Im Folgenden werden die Service-Endpunkte und -kontingente für diesen Service beschrieben. Um programmgesteuert eine Verbindung zu einem herzustellen AWS-Service, verwenden Sie einen Endpunkt. Zusätzlich zu den AWS Standardendpunkten AWS-Services bieten einige FIPS-Endpunkte in ausgewählten Regionen. Weitere Informationen finden Sie unter AWS -Service-Endpunkte. Service Quotas, auch als Limits bezeichnet, sind die maximale Anzahl von Serviceressourcen oder -vorgängen für Ihr AWS-Konto. Weitere Informationen finden Sie unter AWS -Servicekontingente.

Service-Endpunkte

Die Amazon EVS-API bietet regionale und Dual-Stack-Endpunkte sowie FIPS-Endpunkte für US-Regionen. Informationen zur Verwendung der Dual-Stack-Endpunkte mit dem finden Sie in der Konfiguration der AWS CLIDual-Stack- und FIPS-Endgeräte im Tools-Referenzhandbuch. AWS SDKs

Name der Region	Region	Endpunkt	Protokoll
USA Ost (Nord-Virginia)	us-east-1	evs.us-east-1.amazonaws.com evs-fips.us-east-1.amazonaws.com evs.us-east-1.api.aws evs-fips.us-east-1.api.aws	HTTPS
USA Ost (Ohio)	us-east-2	evs.us-east-2.amazonaws.com evs-fips.us-east-2.amazonaws.com evs.us-east-2.api.aws	HTTPS

Name der Region	Region	Endpunkt	Protokoll
		evs-fips.us-east-2.api.aws	
USA West (Oregon)	us-west-2	evs.us-west-2.amazonaws.com evs-fips.us-west-2.amazonaws.com evs.us-west-2.api.aws evs-fips.us-west-2.api.aws	HTTPS
Asien-Pazifik (Tokio)	ap-northeast-1	evs.ap-northeast-1.amazonaws.com evs.ap-northeast-1.api.aws	HTTPS
Europa (Frankfurt)	eu-central-1	evs.eu-central-1.amazonaws.com evs.eu-central-1.api.aws	HTTPS
Europa (Irland)	eu-west-1	evs.eu-west-1.amazonaws.com evs.eu-west-1.api.aws	HTTPS

Servicekontingente

Important

Um die Erstellung einer Amazon EVS-Umgebung zu aktivieren, muss Ihre Hostanzahl pro EVS-Umgebungskontingent mindestens 4 betragen. Das Standardkontingent ist 0. Um dieses Kontingent zu erhöhen, rufen Sie die Konsole Service Quotas auf und fordern Sie eine Erhöhung des Kontingents an.

Note

Wenn Sie EC2 Dedicated Hosts für Ihre Amazon EVS-Umgebung verwenden möchten, stellen Sie sicher, dass Ihr EC2 Dedicated Host-Kontingent die Anzahl der Dedicated Hosts

widerspiegelt, die Sie für eine gewünschte Region verwenden möchten. VCF-Bereitstellungen erfordern mindestens 4 Hosts. Weitere Informationen finden Sie unter Amazon EC2 Dedicated Hosts.

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 Management Console 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.

Name	Standard	Anpassbar	Beschreibung
Anzahl der Hosts pro EVS-Umgebung	0	Ja	Maximale Anzahl von Hosts, die in einer einzigen Amazon EVS-Umgebung bereitgestellt werden können.

Dokumentenverlauf für das Amazon Elastic VMware Service User Guide

> **Note**
>
> Amazon EVS befindet sich in der öffentlichen Vorschauversion und kann sich ändern.

In der folgenden Tabelle werden die Dokumentationsversionen für Amazon Elastic VMware Service beschrieben.

Änderung	Beschreibung	Datum
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.