aws

Guida per l'utente

Amazon Elastic VMware Service

Amazon Elastic VMware Service: Guida per l’utente

Table of Contents

Cos'è Amazon Elastic VMware Service?

Puoi utilizzare Amazon Elastic VMware Service (Amazon EVS) per distribuire ed eseguire un ambiente VMware Cloud Foundation (VCF) direttamente su istanze EC2 bare metal all'interno Amazon Virtual Private Cloud (VPC).

Argomenti

Caratteristiche di Amazon EVS

Le seguenti sono le caratteristiche principali di Amazon EVS:

Semplifica e accelera la migrazione verso AWS

Elimina gli ostacoli legati alla migrazione e garantisci la coerenza operativa con la portabilità dell'abbonamento e l'implementazione automatizzata di VMware Cloud Foundation (VCF) nel cloud. Estendi le reti locali e migra i carichi di lavoro senza dover cambiare gli indirizzi IP, riqualificare il personale o riscrivere i runbook operativi.

Mantieni il controllo della tua architettura nel cloud VMware

Mantieni il controllo completo sulla tua VMware architettura e ottimizza uno stack di virtualizzazione che soddisfi le esigenze specifiche delle tue applicazioni, inclusi componenti aggiuntivi e soluzioni di terze parti.

Gestisci autonomamente o sfrutta i partner per un'esperienza AWS gestita

Sfrutta la scelta e la flessibilità necessarie per l'autogestione oppure sfrutta l'esperienza dei AWS partner per gestire e utilizzare l'ambiente VCF AWS al fine di raggiungere gli obiettivi aziendali in termini di talento, tempo e costi.

Scalate e proteggete la vostra azienda dalle interruzioni

Migliora la scalabilità sul cloud più sicuro, scalabile e resiliente per la migrazione e il funzionamento dei tuoi carichi di lavoro basati. VMware

Abbraccia l' AWS innovazione per trasformare le tue applicazioni e la tua infrastruttura

Come servizio AWS nativo, Amazon EVS semplifica l'estensione e l'espansione del tuo VMware ambiente con oltre 200 servizi (inclusi database gestiti, analisi, serverless e container e intelligenza artificiale generativa) per trasformare il tuo business.

Inizia a usare Amazon EVS

Per creare il tuo primo ambiente Amazon EVS, consultaNozioni di base. In generale, per iniziare a usare Amazon EVS è necessario completare i seguenti passaggi.

1. Completare i prerequisiti Per ulteriori informazioni, consulta Configurazione di Amazon Elastic VMware Service.
2. Crea un ambiente Amazon EVS. Durante la creazione dell'ambiente, Amazon EVS crea le sottoreti VLAN richieste utilizzando gli intervalli CIDR specificati e aggiunge host all'ambiente.
3. Personalizza VCF. Configura il tuo ambiente nell'interfaccia utente vSphere in base alle tue esigenze. Ciò può includere la configurazione di accessi, policy, monitoraggio e altro.
4. Connect e migra. Connect il tuo ambiente al tuo data center locale e migra i tuoi carichi di lavoro VCF su Amazon EVS.

Accesso ad Amazon EVS

Puoi definire e configurare le tue distribuzioni Amazon EVS utilizzando le seguenti interfacce:

- Console Amazon EVS: fornisce un'interfaccia Web per creare ambienti Amazon EVS.
- AWS CLI - Fornisce comandi per un ampio set di Servizi AWS ed è supportato su Windows, macOS e Linux. Per ulteriori informazioni, consulta AWS Command Line Interface.
- AWS CloudFormation - Fornisce una specifica per ogni tipo di risorsa, ad esempio`AWS::EVS::Environment`. Crei un modello utilizzando le specifiche delle risorse e ti CloudFormation occupi del provisioning e della configurazione delle risorse per te.

Concetti e componenti di Amazon EVS

Questa sezione spiega alcuni concetti e componenti chiave di Amazon EVS.

Ambiente Amazon EVS

Un ambiente Amazon EVS è un contenitore logico per risorse VMware Cloud Foundation (VCF), come host vSphere, vSAN, NSX e SDDC Manager. Un ambiente contiene un dominio VCF consolidato con un cluster vSphere che ospita i componenti per la gestione, il monitoraggio e l'istanza dello stack software VCF. Ogni ambiente è mappato direttamente a un'appliance SDDC Manager. Per ulteriori informazioni, consulta the section called "Architecture".

Host Amazon EVS

Un host Amazon EVS è un host VMware ESX che viene eseguito su istanze Amazon EC2 bare metal. Gli host Amazon EVS utilizzano volumi di NVMe istanze locali per i datastore vSAN, che archiviano le macchine virtuali di gestione e carico di lavoro.

> **Warning**
>
> I volumi dell'Instance Store sono effimeri. I dati archiviati su questi volumi non persistono se l'istanza EC2 sottostante viene interrotta o terminata. L'arresto o la chiusura Amazon EC2 delle istanze utilizzate da Amazon EVS senza scomissioni all'interno di VCF può causare la perdita di dati.
>
> Per ulteriori informazioni sulla manutenzione dell'host, consulta. the section called "Manutenzione degli host"

Sottorete di accesso al servizio

La sottorete di accesso al servizio è una sottorete VPC standard che consente ad Amazon EVS di accedere alla distribuzione VCF. Durante la creazione dell'ambiente Amazon EVS, specifichi il VPC e la sottorete che Amazon EVS deve utilizzare per l'accesso al servizio.

Quando crei un ambiente Amazon EVS, Amazon EVS fornisce interfacce di rete elastiche nella sottorete di accesso al servizio per facilitare la connettività di gestione alle appliance VCF e agli host ESX. Questa connettività è necessaria per consentire ad Amazon EVS di implementare, gestire e monitorare la distribuzione VCF.

Sottorete VLAN Amazon EVS

Una sottorete VLAN Amazon EVS è una sottorete Amazon VPC gestita da Amazon EVS. Le sottoreti VLAN forniscono connettività VPC per host Amazon EVS e appliance VCF come VMware NSX, HCX e vCenter Server. VMware VMware Ogni sottorete VLAN dispone di un tag VLAN per consentire la segmentazione logica del traffico di rete VLAN.

Amazon EVS crea tutte le sottoreti VLAN utilizzate dal servizio quando viene creato l'ambiente Amazon EVS. Fornisci gli input di blocco CIDR utilizzati dalle sottoreti VLAN. È necessario assicurarsi che i blocchi CIDR della sottorete VLAN siano dimensionati correttamente in base al numero di host che verranno configurati, tenendo conto delle future esigenze di scalabilità. I blocchi CIDR devono avere una dimensione minima di /28 netmask e una dimensione massima di /24 netmask. I blocchi CIDR non devono sovrapporsi a nessun blocco CIDR esistente associato al VPC.

Al momento della creazione, le sottoreti VLAN vengono associate implicitamente alla tabella di routing principale del VPC. Dopo l'implementazione è possibile associare in modo esplicito le sottoreti VLAN a una tabella di routing personalizzata. Per ulteriori informazioni, consulta the section called "Considerazioni sulla rete Amazon EVS".

> **Important**
>
> Le sottoreti VLAN Amazon EVS possono essere create solo durante la creazione dell'ambiente Amazon EVS e non possono essere modificate dopo la creazione dell'ambiente. È necessario assicurarsi che i blocchi CIDR della sottorete VLAN siano dimensionati correttamente prima di creare l'ambiente. Non sarà possibile aggiungere sottoreti VLAN dopo la distribuzione dell'ambiente.

> **Important**
>
> Le regole dei gruppi di sicurezza EC2 non vengono applicate alle interfacce di rete elastiche di Amazon EVS collegate alle sottoreti VLAN. Per controllare il traffico da e verso le sottoreti VLAN, è necessario utilizzare una lista di controllo degli accessi alla rete.

Sottorete VLAN di gestione dell'host

La sottorete VLAN di gestione degli host separa il traffico di gestione dal traffico degli utenti e consente la gestione remota degli host. L'interfaccia di rete vmkernel per la gestione degli host EVS si connette a questa sottorete.

Sottorete VLAN VMotion

La sottorete VLAN vMotion segmenta logicamente il traffico vMotion e viene utilizzata durante un processo VMware vMotion per spostare macchine virtuali tra host.

Sottorete VLAN vSAN

La sottorete VLAN vSAN viene utilizzata da vSAN per separare il traffico relativo alle VMware operazioni di storage di vSAN da altro traffico di rete.

Sottorete VLAN VTEP

La sottorete VLAN VTEP utilizza gli endpoint del tunnel virtuale VMware NSX (VTEP) per incapsulare e decapsulare il traffico di rete overlay per gli host Amazon EVS ESX.

Sottorete VLAN Edge VTEP

La sottorete VLAN Edge VTEP è una sottorete VLAN VTEP specializzata dedicata al traffico di overlay dell'appliance NSX Edge. Questa VLAN viene utilizzata per la comunicazione overlay tra i edge NSX e gli host ESX.

Sottorete VLAN di gestione (VM)

La sottorete Management VM VLAN viene utilizzata per la gestione di appliance virtuali, tra cui NSX Manager, vCenter Server e SDDC Manager.

Sottorete VLAN HCX uplink

La sottorete VLAN uplink HCX viene utilizzata per la comunicazione tra i dispositivi HCX Interconnect (HCX-IX) e HCX Network Extension (HCX-NE) e consente la creazione dell'uplink HCX service mesh.

Sottorete VLAN NSX uplink

La sottorete VLAN uplink NSX viene utilizzata per connettere le reti overlay NSX al resto del VPC e a qualsiasi altra rete esterna configurata. La sottorete VLAN uplink NSX è configurata sugli uplink del nodo NSX Edge.

Sottorete VLAN di espansione

La sottorete VLAN di espansione può essere utilizzata per abilitare funzioni aggiuntive supportate da VCF, come NSX Federation. Amazon EVS crea due sottoreti VLAN di espansione durante la creazione dell'ambiente.

VMware NSX

VMware NSX è una piattaforma SDN (Software-Defined Networking) che consente la virtualizzazione della rete. Amazon EVS utilizza VMware NSX per creare e gestire la rete overlay su cui vengono eseguiti i carichi di lavoro e le appliance VMware Cloud Foundation (VCF). Amazon EVS implementa un paio di nodi Active/Standby NSX Edge, insieme a una rete overlay NSX. Amazon EVS configura automaticamente tutti i routing e gli uplink NSX per tuo conto come parte della distribuzione. Per ulteriori informazioni sui concetti comuni di NSX, consulta Concetti chiave nella Guida all'installazione di NSX. VMware

Connector

Un connettore Amazon EVS consente ad Amazon EVS di comunicare con le appliance di gestione VMware Cloud Foundation, come un'appliance vCenter Server, nel tuo ambiente. Ogni connettore è mappato a un singolo dispositivo di gestione, che richiede il nome di dominio completo (FQDN) e le credenziali archiviate in un segreto di Secrets Manager AWS per l'autenticazione con l'appliance. Amazon EVS esegue periodicamente controlli di raggiungibilità dell'appliance tramite il connettore. Se il connettore perde la raggiungibilità, le funzionalità che dipendono dal connettore ne risentiranno.

- Per creare un connettore, vedere. the section called “Crea connettore”
- Per aggiornare un connettore, vederethe section called “Aggiorna connettore”.
- Per eliminare un connettore, vederethe section called “Elimina connettore”.

Diritto alla licenza Windows Server per Amazon EVS

Il diritto alla licenza Windows Server per Amazon EVS consente alle macchine virtuali (VMs) in esecuzione nel tuo ambiente Amazon EVS di utilizzare AWS le licenze Windows Server offerte. I diritti di licenza di Windows Server sono offerti per vCPU all'ora con un modello. pay-as-you-go

Per utilizzare i diritti di licenza di Windows Server, devi prima creare un connettore per stabilire la raggiungibilità tra Amazon EVS e la tua appliance vCenter Server. Il controllo di raggiungibilità sul connettore deve essere superato prima di poter creare un'autorizzazione.

Amazon EVS utilizza il connettore vCenter per monitorare gli eventi del ciclo di vita delle macchine virtuali per i titolari. VMs Se il connettore perde la raggiungibilità, le autorizzazioni associate entrano in uno stato di rischio. Se la raggiungibilità non viene ripristinata entro un periodo di prova di 8 ore, le autorizzazioni vengono annullate e il monitoraggio dell'utilizzo delle licenze viene interrotto dal momento in cui l'autorizzazione è entrata nello stato di rischio.

Dopo aver creato un'autorizzazione e aver attivato una macchina virtuale, Amazon EVS inizia a monitorare l'utilizzo della licenza Windows Server della macchina virtuale corrispondente. Se la macchina virtuale è spenta o le vCPU configurate vengono scalate verso l'alto o verso il basso in base alla richiesta, si paga la licenza solo per le ore totali di vCPU utilizzate.

> **Warning**
>
> I sistemi operativi guest supportati sono Windows Server 2016 e versioni successive.

Per istruzioni, consulta the section called “Crea connettore” e the section called “Crea un'autorizzazione”.

Dopo aver creato i permessi, puoi configurare ogni macchina virtuale Windows Server per l'attivazione tramite un endpoint VPC. Per istruzioni, consulta the section called “Configurare l'attivazione di Windows Server”.

VMware Estensione del cloud ibrido (HCX)

VMware Hybrid Cloud Extension (VMware HCX) è una piattaforma di mobilità delle applicazioni progettata per semplificare la migrazione delle applicazioni, riequilibrare i carichi di lavoro e ottimizzare il disaster recovery tra data center e cloud. Puoi usare HCX per migrare i tuoi carichi di lavoro VMware basati su Amazon EVS.

Puoi configurare la connettività per VMware HCX utilizzando Direct Connect un gateway di transito associato o utilizzando un allegato VPN a un AWS Site-to-Site gateway di transito. Per ulteriori informazioni, consulta Migrazione.

Architettura Amazon EVS

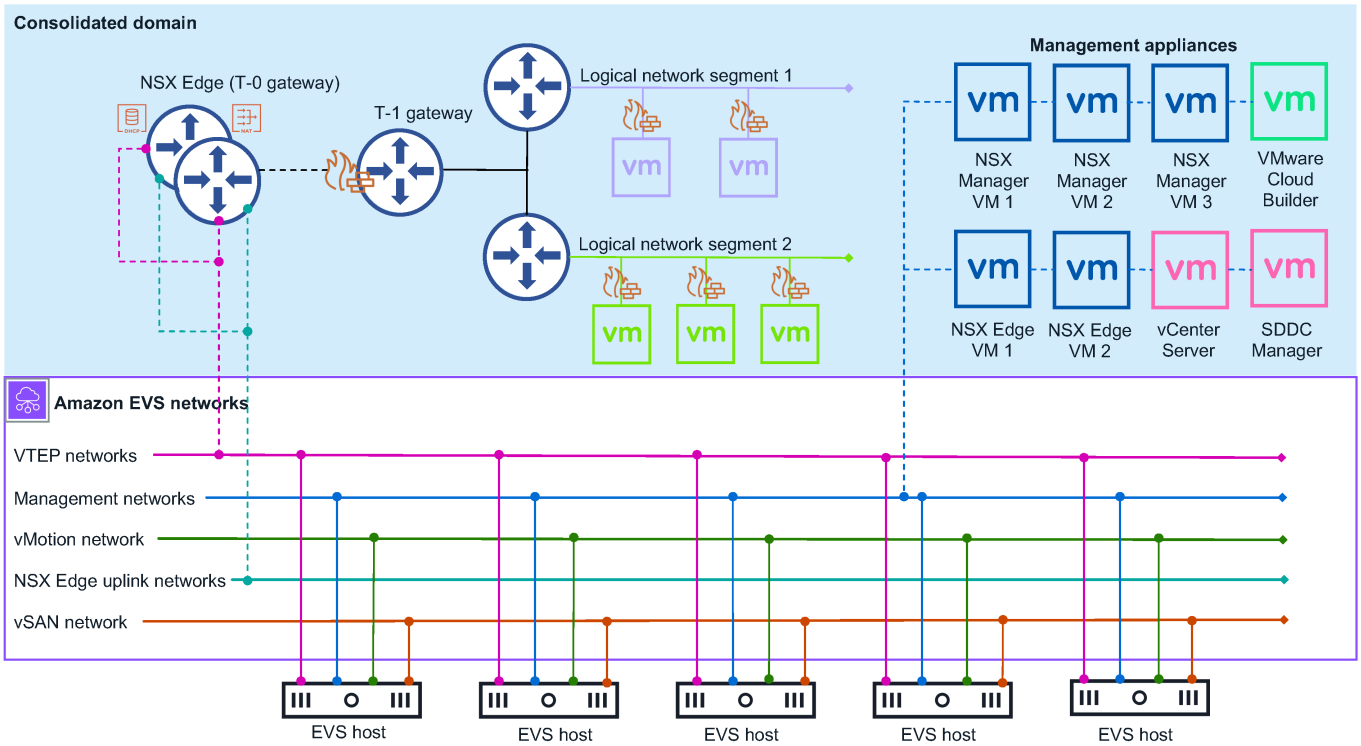
Amazon EVS implementa un modello di architettura consolidata VMware Cloud Foundation (VCF). In questo modello, i componenti di gestione VCF e i carichi di lavoro dei clienti vengono eseguiti insieme

su un dominio consolidato. L'ambiente Amazon EVS è gestito da un singolo vCenter Server con pool di risorse vSphere che garantiscono l'isolamento tra la gestione e i carichi di lavoro dei clienti.

Il dominio consolidato distribuito da Amazon EVS contiene i seguenti componenti di gestione VCF:

- Host ESX
- istanza di vCenter Server
- Gestore SDDC
- Datastore vSAN
- Three-node Cluster NSX Manager
- Cluster vSphere
- Cluster NSX Edge

Il diagramma seguente mostra un esempio di architettura Amazon EVS che è stata implementata in un ambiente Amazon EVS e mostra come i componenti dell'ambiente sono collegati. Nel diagramma, l'ambiente Amazon EVS con un'architettura di dominio consolidata è ombreggiato in blu. La topologia di rete Amazon EVS sottostante è illustrata all'interno di una linea viola continua.



Topologia di rete

Un ambiente Amazon EVS ha due livelli di rete di gestione separati:

Amazon VPC

Le sottoreti VLAN Amazon VPC e Amazon EVS create nel VPC durante la creazione dell'ambiente costituiscono la rete sottostante per la distribuzione VCF. Questa infrastruttura fornisce connettività per reti overlay NSX, gestione host, VMotion e VSAN. Amazon VPC Route Server consente il routing dinamico tra la rete overlay e le reti overlay. Per ulteriori informazioni, consulta the section called "Concetti e componenti".

> **Note**
>
> Le sottoreti VLAN di Amazon EVS vengono utilizzate solo per facilitare la comunicazione overlay VCF. Le macchine virtuali guest che eseguono i carichi di lavoro dei clienti devono essere distribuite su reti overlay NSX. La distribuzione di macchine virtuali guest sulla sottorete di subnet VLAN di Amazon EVS non è supportata.

Rete overlay VMware NSX

Amazon EVS configura una rete overlay NSX per tuo conto come parte della distribuzione. Puoi configurare reti overlay NSX aggiuntive per ottenere l'isolamento di rete tra diversi carichi di lavoro o applicazioni all'interno del tuo ambiente Amazon EVS. Per ulteriori informazioni, consulta Overlay Design for VMware Cloud Foundation nella documentazione del prodotto VMware Cloud Foundation.

> **Note**
>
> Amazon EVS supporta solo un gateway tier-0 per un cluster NSX Edge con due nodi Active/Standby NSX Edge. Questo gateway tier-0 si connette e pubblicizza tutte le reti overlay configurate per l'uso con Amazon EVS.

I due livelli di rete sono collegati da un cluster NSX Edge con due nodi Active/Standby NSX Edge. I nodi NSX Edge consentono la comunicazione tramite VPC tra macchine virtuali nelle VLAN, nonché

la connettività Internet e la connettività privata Direct Connect utilizzando AWS Site-to-Site una VPN con un gateway di transito.

Considerazioni sulla rete Amazon EVS

La rete di gestione richiede le seguenti configurazioni delle risorse di rete. Fornisci questi input durante la creazione dell'ambiente Amazon EVS. Per ulteriori informazioni, consulta the section called "Concetti e componenti".

- Un Amazon VPC. Assicurati che il blocco CIDR VPC IPv4 sia dimensionato in modo appropriato per ospitare la sottorete VPC richiesta e le sottoreti VLAN Amazon EVS utilizzate da Amazon EVS durante la creazione dell'ambiente. Per ulteriori informazioni, consulta the section called "Sottorete VLAN Amazon EVS".

  > **Note**
  >
  > Amazon EVS non supporta al momento IPv6.

- Una sottorete di accesso ai servizi nel tuo VPC. Amazon EVS utilizza questa sottorete per mantenere una connessione persistente all'appliance SDDC Manager. Per ulteriori informazioni, consulta the section called "Sottorete di accesso al servizio".

  > **Note**
  >
  > Al momento Amazon EVS supporta solo Single-AZ le implementazioni. Tutte le sottoreti VPC utilizzate da Amazon EVS devono esistere in un'unica zona di disponibilità in una regione in cui il servizio è disponibile.

  > **Note**
  >
  > Tutte le sottoreti VPC richiedono tabelle di routing associate configurate in base ai requisiti di rete dell'organizzazione.

- Un indirizzo IP del server DNS primario e un indirizzo IP del server DNS secondario nell'insieme di opzioni DHCP del VPC per risolvere gli indirizzi IP dell'host. Amazon EVS richiede inoltre la creazione di una zona di ricerca diretta DNS con record A e una zona di ricerca inversa con record PTR per ogni appliance di gestione VCF e host Amazon EVS nella distribuzione. Per ulteriori informazioni, consulta the section called "Configurare i server DNS".

- Blocchi CIDR della sottorete VLAN di Amazon EVS per ogni sottorete VLAN fornita da Amazon EVS durante la creazione dell'ambiente. I blocchi CIDR devono avere una dimensione minima di /28 netmask e una dimensione massima di /24 netmask. I blocchi CIDR non devono essere sovrapposti.
- Un'istanza di Amazon VPC Route Server con la propagazione del Route Server abilitata.
- Due endpoint Route Server nella sottorete di accesso al servizio.
- Due peer di Route Server che eseguono il peering dei nodi NSX Edge di cui Amazon EVS effettua il provisioning con gli endpoint Route Server.

Tier-0 gateway

Il gateway tier-0 gestisce tutto il traffico nord-sud tra le reti logiche e fisiche e viene creato sulla rete overlay NSX. Questo gateway tier-0 viene creato come parte della distribuzione di Amazon EVS.

> **Note**
>
> Amazon EVS supporta solo un gateway tier-0 per un cluster NSX Edge con due nodi Active/Standby NSX Edge.

Tier-1 gateway

Il gateway tier-1 gestisce il traffico est-ovest tra i segmenti di rete instradati all'interno di un ambiente e viene creato sulla rete overlay NSX. Il gateway tier-1 dispone di connessioni in downlink ai segmenti e connessioni uplink al gateway tier-0. È possibile creare e configurare gateway aggiuntivi se necessario. Tier-1

Cluster NSX Edge

Amazon EVS utilizza l'interfaccia NSX Manager per distribuire un cluster NSX Edge con due nodi NSX Edge eseguiti in modalità. Active/Standby Questo cluster NSX Edge fornisce la piattaforma su cui vengono eseguiti i Tier-1 gateway Tier-0 e le connessioni VPN IPSec e il relativo meccanismo di routing BGP.

Risorse Amazon EVS

Amazon EVS fornisce le seguenti AWS risorse durante la creazione dell'ambiente. Queste risorse vengono visualizzate nel VPC a cui consenti ad Amazon EVS di accedere e sono visibili durante Console di gestione AWS e AWS CLI dopo la loro creazione.

> **Important**
>
> La modifica di queste risorse al di fuori della console e dell'API di Amazon EVS potrebbe influire sulla disponibilità e sulla stabilità del tuo ambiente Amazon EVS.

- Interfacce di rete elastiche di Amazon EVS che consentono la connettività ai dispositivi e agli host VCF.
- Host Amazon EVS ESX eseguiti su istanze Amazon EC2 bare metal. Per ulteriori informazioni, consulta the section called "Host Amazon EVS".

  > **Important**
  >
  > Il tuo ambiente Amazon EVS deve avere un minimo di 4 host e non più di 32 host. Amazon EVS supporta solo ambienti con 4-32 host.

- Sottoreti VLAN Amazon EVS che collegano il tuo VPC ai dispositivi VCF. Per ulteriori informazioni, consulta the section called "Sottorete VLAN Amazon EVS".

Configurazione di Amazon Elastic VMware Service

Per utilizzare Amazon EVS, dovrai configurare altri AWS servizi e configurare il tuo ambiente per soddisfare i requisiti di VMware Cloud Foundation (VCF). Per un elenco di controllo riassuntivo dei prerequisiti di implementazione, consulta. the section called "Lista di controllo per l'implementazione"

Argomenti

Registrati per un AWS account

Per iniziare AWS, hai bisogno di un AWS account. Per informazioni sulla creazione di un AWS account, consulta Guida introduttiva a un AWSAWS account nella Guida di riferimento alla gestione degli account.

Crea un ruolo IAM per delegare l'autorizzazione Amazon EVS a un utente IAM

Puoi utilizzare i ruoli per delegare l'accesso alle tue risorse. AWS Con i ruoli IAM, puoi stabilire relazioni di fiducia tra il tuo account fiduciario e altri account AWS affidabili. L'account affidabile possiede la risorsa a cui accedere e l'account affidabile contiene gli utenti che devono accedere alla risorsa.

Dopo aver creato la relazione di trust, un utente IAM o un'applicazione dell'account affidabile può utilizzare l'operazione `AssumeRole` API AWS Security Token Service (AWS STS). Questa operazione fornisce credenziali di sicurezza temporanee che consentono l'accesso alle AWS risorse del tuo account. Per ulteriori informazioni, consulta Creare un ruolo per delegare le autorizzazioni a un utente IAM nella Guida per l'utente. AWS Identity and Access Management

Segui questi passaggi per creare un ruolo IAM con una politica di autorizzazioni che consenta l'accesso alle operazioni di Amazon EVS.

> **Note**
>
> Amazon EVS non supporta l'uso di un profilo di istanza per passare un ruolo IAM a un'istanza EC2.

Example

IAM console

1. Vai alla console IAM.
2. Nel menu a sinistra, scegli Politiche.
3. Scegli Crea policy.
4. Nell'editor delle politiche, crea una politica di autorizzazioni che abiliti le operazioni di Amazon EVS. Per un esempio di policy, consulta the section called "Crea e gestisci un ambiente Amazon EVS". Per visualizzare tutte le azioni, le risorse e le chiavi di condizione di Amazon EVS disponibili, consulta Azioni nel Service Authorization Reference.
5. Scegli Next (Successivo).
6. In Nome della politica, inserisci un nome di politica significativo per identificare questa politica.

7. Rivedi le autorizzazioni definite in questa politica.
8. (Facoltativo) Aggiungi tag per identificare, organizzare o cercare questa risorsa.
9. Scegli Crea policy.
10. Nel menu a sinistra, scegli Ruoli.
11. Scegli Crea ruolo.
12. Per Tipo di entità attendibile, scegli Account AWS.
13. In An Account AWS , specifica l'account su cui desideri eseguire le azioni Amazon EVS e scegli Avanti.
14. Nella pagina Aggiungi autorizzazioni, seleziona la politica di autorizzazione che hai creato in precedenza e scegli Avanti.
15. In Nome ruolo, inserisci un nome significativo per identificare questo ruolo.
16. Esamina la politica di fiducia e assicurati che quella corretta Account AWS sia elencata come principale.
17. (Facoltativo) Aggiungi tag per identificare, organizzare o cercare questa risorsa.
18. Scegli Crea ruolo.

AWS CLI

1. Copia i seguenti contenuti in un file JSON di policy di fiducia. Per l'ARN principale, sostituisci l'ID e il `service-user` nome di esempio con il tuo Account AWS Account AWS ID e il tuo nome utente IAM.

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

2. Crea il ruolo. `evs-environment-role-trust-policy.json`Sostituiscilo con il nome del file della politica di fiducia.

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

3. Crea una politica di autorizzazioni che abiliti le operazioni di Amazon EVS e associa la policy al ruolo. Sostituisci `myAmazonEVSEnvironmentRole` con il nome del tuo ruolo. Per un esempio di policy, consulta the section called "Crea e gestisci un ambiente Amazon EVS". Per visualizzare tutte le azioni, le risorse e le chiavi di condizione di Amazon EVS disponibili, consulta Azioni nel Service Authorization Reference.

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

Registrati per un AWS Affari, AWS Enterprise On-Ramp o AWS Piano Enterprise Support

Amazon EVS richiede che i clienti siano iscritti a un piano AWS Business On-Ramp, AWS Enterprise o Enterprise AWS Support per ricevere accesso continuo al supporto tecnico e alla guida architetturale. AWS Business Support è il livello di AWS supporto minimo che soddisfa i requisiti di Amazon EVS. Se hai carichi di lavoro critici per l'azienda, ti consigliamo di iscriverti ai piani On-Ramp Enterprise AWS o Enterprise AWS Support. Per ulteriori informazioni, consulta Compare AWS Support Plans.

> **Important**
>
> La creazione dell'ambiente Amazon EVS non riesce se non ti iscrivi a un piano AWS Business On-Ramp, AWS Enterprise o AWS Enterprise Support.

Controlla le quote

Per consentire la creazione dell'ambiente Amazon EVS, assicurati che il tuo account disponga delle quote minime richieste a livello di account. Per ulteriori informazioni, consulta Service Quotas.

> **Important**
>
> La creazione dell'ambiente Amazon EVS non riesce se il numero di host per valore di quota dell'ambiente EVS non è almeno 4.

Pianifica le dimensioni del VPC CIDR

Quando crei un ambiente Amazon EVS, devi specificare un blocco CIDR VPC. Il blocco VPC CIDR non può essere modificato dopo la creazione dell'ambiente e dovrà disporre di spazio sufficiente per ospitare le sottoreti e gli host EVS richiesti che Amazon EVS crea durante la distribuzione dell'ambiente. Di conseguenza, è fondamentale pianificare attentamente la dimensione del blocco CIDR, tenendo conto dei requisiti di Amazon EVS e delle future esigenze di scalabilità prima della distribuzione. Amazon EVS richiede un blocco CIDR VPC con una dimensione minima di /22 netmask per consentire spazio sufficiente per le sottoreti e gli host EVS richiesti. Per ulteriori informazioni, consulta the section called “Considerazioni sulla rete Amazon EVS”.

> **Important**
>
> Assicurati di disporre di uno spazio di indirizzi IP sufficiente sia per la sottorete VPC che per le sottoreti VLAN create da Amazon EVS per le appliance VCF. Il blocco VPC CIDR deve avere una dimensione minima di /22 netmask per consentire spazio sufficiente per le sottoreti e gli host EVS richiesti.

> **Note**
>
> Amazon EVS non supporta al momento IPv6.

Crea un VPC con sottoreti

Amazon EVS implementa il tuo ambiente in un VPC fornito da te. Questo VPC deve contenere una sottorete per l'accesso al servizio Amazon EVS (). the section called “Sottorete di accesso al servizio” Per i passaggi per creare un VPC con sottoreti per Amazon EVS, consulta. the section called “Crea un VPC con sottoreti e tabelle di routing”

Configurare la tabella di routing principale del VPC

Le sottoreti VLAN di Amazon EVS sono associate implicitamente alla tabella di routing principale del VPC. Per abilitare la connettività a servizi dipendenti come DNS o sistemi locali per una corretta implementazione dell'ambiente, è necessario configurare la tabella di routing principale per consentire il traffico verso questi sistemi. Per ulteriori informazioni, consulta the section called "Associa esplicitamente le sottoreti VLAN di Amazon EVS a una tabella di routing VPC".

> **Important**
>
> Amazon EVS supporta l'uso di una tabella di routing personalizzata solo dopo la creazione dell'ambiente Amazon EVS. Le tabelle di routing personalizzate non devono essere utilizzate durante la creazione dell'ambiente Amazon EVS, poiché ciò potrebbe causare problemi di connettività.

Requisiti del percorso del gateway

Configura i percorsi per questi tipi di gateway in base ai tuoi requisiti di connettività:

- Gateway NAT (NGW)
  - Opzionale per l'accesso a Internet solo in uscita.
  - Deve trovarsi in una sottorete pubblica con accesso tramite gateway Internet.
  - Aggiungi percorsi da sottoreti private e sottoreti VLAN EVS al gateway NAT.
  - Per ulteriori informazioni, consulta Lavora con i gateway NAT nella Amazon VPC User Guide.
- Transit Gateway (TGW)
  - Necessario per la connettività locale tramite AWS Direct Connect e AWS Site-to-Site VPN.
  - Aggiungi percorsi per intervalli di rete locali.
  - Configura la propagazione delle rotte se usi BGP.
  - Per ulteriori informazioni, consulta Transit Gateway in Amazon VPC Transit Gateways nella Amazon VPC User Guide.

Best practice

- Documenta tutte le configurazioni delle tabelle di routing.

- Usa convenzioni di denominazione coerenti.
- Controlla regolarmente le tabelle delle rotte.
- Verifica la connettività dopo aver apportato le modifiche.
- Esegui il backup delle configurazioni della tabella dei percorsi.
- Monitora lo stato e la propagazione delle rotte.

Per ulteriori informazioni sull'utilizzo delle tabelle di routing, consulta Configure route tables nella Amazon VPC User Guide.

Configura il set di opzioni DHCP del tuo VPC

Important

L'implementazione del tuo ambiente fallisce se non soddisfi questi requisiti di Amazon EVS:

- Includi un indirizzo IP del server DNS primario e un indirizzo IP del server DNS secondario nel set di opzioni DHCP.
- Includi una zona di ricerca diretta DNS con record A per ogni appliance di gestione VCF e host Amazon EVS nella tua distribuzione.
- Includi una zona di ricerca inversa DNS con record PTR per ogni appliance di gestione VCF e host Amazon EVS nella tua distribuzione.
- Configura la tabella di routing principale del VPC per assicurarti che esista un percorso verso i tuoi server DNS.
- Assicurati che la registrazione del nome di dominio sia valida e non sia scaduta e che non esistano nomi host o indirizzi IP duplicati.
- Configura i gruppi di sicurezza e le liste di controllo degli accessi alla rete (ACL) per consentire ad Amazon EVS di comunicare con:
  - Server DNS sulla porta 53. TCP/UDP
  - Sottorete VLAN di gestione dell'host tramite HTTPS e SSH.
  - Sottorete VLAN di gestione tramite HTTPS e SSH.

Per ulteriori informazioni, consulta the section called “Configurazione dei server DNS e NTP utilizzando il set di opzioni VPC DHCP”.

Crea e configura l'infrastruttura VPC Route Server

Amazon EVS utilizza Amazon VPC Route Server per BGP-based abilitare il routing dinamico verso la tua rete VPC underlay. È necessario specificare un server di routing che condivida le rotte verso almeno due endpoint del server di routing nella sottorete di accesso al servizio. L'ASN peer configurato sui peer del server di routing deve corrispondere e gli indirizzi IP peer devono essere univoci.

Important

L'implementazione del tuo ambiente fallisce se non soddisfi questi requisiti di Amazon EVS per la configurazione del VPC Route Server:

- È necessario configurare almeno due endpoint del server di routing nella sottorete di accesso al servizio.
- Quando si configura Border Gateway Protocol (BGP) per il Tier-0 gateway, il valore ASN peer di VPC Route Server deve corrispondere al valore ASN peer di NSX Edge.
- Quando si creano i due peer del server di routing, è necessario utilizzare un indirizzo IP univoco dalla VLAN uplink NSX per ogni endpoint. Questi due indirizzi IP verranno assegnati ai bordi NSX durante l'implementazione dell'ambiente Amazon EVS.
- Quando abiliti la propagazione del Route Server, devi assicurarti che tutte le tabelle di routing che vengono propagate abbiano almeno un'associazione di sottorete esplicita. La pubblicità delle rotte BGP fallisce se le tabelle di routing propagate non hanno un'associazione di sottorete esplicita.

Note

Per il rilevamento della peer liveness di Route Server, Amazon EVS supporta solo il meccanismo keepalive BGP predefinito. Amazon EVS non supporta il rilevamento dell'inoltro bidirezionale (BFD) multi-hop.

Prerequisiti

Prima di iniziare è necessario disporre di quanto segue:

- Una sottorete VPC per il server di routing.
- Autorizzazioni IAM per gestire le risorse del VPC Route Server.
- Un valore ASN BGP per il server di routing (ASN). Amazon-side Questo valore deve essere compreso nell'intervallo tra 1 e 4294967295.
- Un ASN peer-to-peer per il peer server di routing con il gateway NSX. Tier-0 I valori ASN peer inseriti nel server di routing e nel gateway NSX devono corrispondere. Tier-0 L'ASN predefinito per un'appliance NSX Edge è 65000.

Fasi

Per i passaggi per configurare il Route Server VPC, consulta il tutorial introduttivo di Route Server.

> **Note**
>
> Se utilizzi un gateway NAT o un gateway di transito, assicurati che il server di routing sia configurato correttamente per propagare le route NSX alle tabelle di routing VPC.

> **Note**
>
> Ti consigliamo di abilitare le route persistenti per l'istanza del server di routing con una durata persistente compresa tra 1 e 5 minuti. Se abilitata, le rotte verranno conservate nel database di routing del server di routing anche se tutte le sessioni BGP terminano.

> **Note**
>
> Lo stato della connettività BGP sarà inattivo fino a quando l'ambiente Amazon EVS non sarà distribuito e operativo.

Crea un gateway di transito per la connettività locale

È possibile configurare la connettività tra il data center locale e l' AWS infrastruttura utilizzando Direct Connect un gateway di transito associato o utilizzando un allegato AWS Site-to-Site VPN a un gateway di transito. Per ulteriori informazioni, consulta the section called "Configurare la connettività di rete locale (opzionale)".

Crea una prenotazione di capacità Amazon EC2

Amazon EVS lancia le istanze metal Amazon EC2 che sono gli host ESX nel tuo ambiente Amazon EVS. Per assicurarti di avere una capacità sufficiente disponibile quando aggiungi host, ti consigliamo di richiedere una prenotazione di capacità Amazon EC2. Puoi creare una prenotazione della capacità in qualsiasi momento e scegliere quando avviarla. È possibile richiedere una prenotazione di capacità per l'uso immediato oppure è possibile richiedere una prenotazione di capacità per date future. Per ulteriori informazioni, consulta Reserve computing capacity with EC2 On-Demand Capacity Reservations nella Amazon Elastic Compute Cloud User Guide.

Configura il AWS CLI

AWS CLI È uno strumento da riga di comando con cui lavorare Servizi AWS, incluso Amazon EVS. Viene anche utilizzato per autenticare utenti o ruoli IAM per l'accesso all'ambiente di virtualizzazione Amazon EVS e ad altre AWS risorse dal computer locale. Per fornire AWS risorse dalla riga di comando, è necessario ottenere un ID della chiave di AWS accesso e una chiave segreta da utilizzare nella riga di comando. Quindi è necessario configurare queste credenziali nella AWS CLI. Per ulteriori informazioni, consulta Configurare la versione 2 AWS CLI nella Guida per AWS Command Line Interface l'utente.

Crea un Amazon EC2 coppia di chiavi

Amazon EVS utilizza una coppia di Amazon EC2 key pair fornita durante la creazione dell'ambiente per connettersi ai tuoi host. Per creare una coppia di chiavi, segui i passaggi su Crea una coppia di chiavi per la tua Amazon EC2 istanza nella Guida per l' Amazon Elastic Compute Cloud utente.

Prepara il tuo ambiente per VMware Cloud Foundation (VCF)

Prima di distribuire l'ambiente Amazon EVS, l'ambiente deve soddisfare i requisiti dell'infrastruttura VMware Cloud Foundation (VCF). Per i prerequisiti VCF dettagliati, consulta la cartella di lavoro di pianificazione e preparazione nella documentazione del prodotto VMware Cloud Foundation.

È inoltre necessario acquisire familiarità con i requisiti di VCF 5.2.x. Consulta le note di rilascio di VCF 5.2.x per le informazioni di rilascio pertinenti.

> **Note**
>
> Per informazioni sulle versioni VCF fornite da Amazon EVS, consulta. the section called "Versioni VCF e istanze EC2"

Acquisisci le chiavi di licenza VCF

Per utilizzare Amazon EVS, devi fornire una chiave di soluzione VCF e una chiave di licenza vSAN. I requisiti specifici per il numero di core e la capacità vSAN dipendono dal tipo di istanza selezionato. Per i dettagli sulle soglie minime di core e capacità per il tipo di istanza, consulta la sezione the section called "Abbonamenti VCF" dedicata alla configurazione. Per ulteriori informazioni sulle licenze VCF, vedere Gestione delle chiavi di licenza in VMware Cloud Foundation nella VMware Cloud Foundation Administration Guide.

> **Important**
>
> Utilizza l'interfaccia utente SDDC Manager per gestire la soluzione VCF e le chiavi di licenza vSAN. Amazon EVS richiede il mantenimento di una soluzione VCF valida e delle chiavi di licenza vSAN in SDDC Manager per il corretto funzionamento del servizio.

> **Note**
>
> La tua licenza VCF sarà disponibile per Amazon EVS in tutte le AWS regioni per garantire la conformità delle licenze. Amazon EVS non convalida le chiavi di licenza. Per convalidare le chiavi di licenza, visita l'assistenza Broadcom.

Prerequisiti per VMware HCX

Puoi usare VMware HCX per migrare i carichi di lavoro VMware-based esistenti su Amazon EVS. Prima di utilizzare VMware HCX con Amazon EVS, assicurati che le seguenti attività preliminari siano state completate.

> **Note**
>
> Per impostazione predefinita, VMware HCX non è installato nell'ambiente EVS.

- Prima di poter utilizzare VMware HCX con Amazon EVS, è necessario soddisfare i requisiti minimi di network underlay. Per ulteriori informazioni, consulta i requisiti minimi di Network Underlay nella Guida per l'utente di VMware HCX.
- Verificare che VMware NSX sia installato e configurato nell'ambiente. Per ulteriori informazioni, consulta la Guida all'installazione di VMware NSX.
- Assicurarsi che VMware HCX sia attivato e installato nell'ambiente. Per ulteriori informazioni sull'attivazione e l'installazione di VMware HCX, vedere Informazioni introduttive a VMware HCX nella Guida introduttiva a VMware HCX.
- Se è necessaria la connettività Internet HCX, è necessario completare le seguenti attività preliminari:
  - Assicurati che la tua quota IPAM per la lunghezza della maschera di rete del blocco CIDR IPv4 pubblico Amazon-provided contiguo sia /28 o superiore.

    > **Important**
    >
    > Per la connettività Internet HCX, Amazon EVS richiede l'uso del blocco CIDR IPv4 da un pool IPAM pubblico con una lunghezza della maschera di rete pari o superiore a /28. L'uso di qualsiasi blocco CIDR con una lunghezza della maschera di rete inferiore a /28 comporterà problemi di connettività HCX. Per ulteriori informazioni sull'aumento delle quote IPAM, consulta Quote per l'IPAM.

  - Crea un IPAM e un pool IPAM IPv4 pubblico con CIDR con una lunghezza minima della maschera di rete di /28.
  - Alloca almeno due indirizzi IP elastici (EIP) dal pool IPAM per i dispositivi HCX Manager e HCX Interconnect (). HCX-IX Assegna un indirizzo IP elastico aggiuntivo per ogni appliance di rete HCX da distribuire.
  - Aggiungi il blocco CIDR IPv4 pubblico come CIDR aggiuntivo al tuo VPC.

Per ulteriori informazioni sulla configurazione di HCX, vedere e. the section called “Scegli la tua opzione di connettività HCX” the section called “Opzioni di connettività HCX”

Elenco di controllo dei prerequisiti per l'implementazione di Amazon EVS

Questa sezione contiene un elenco di prerequisiti che devono essere completati per consentire una corretta implementazione dell'ambiente Amazon EVS.

Informazioni sulla chiave di licenza VCF

Componente	Description	Requisiti minimi	Valore (i) di esempio
ID del sito	ID del sito fornito da Broadcom per l'accesso al portale di supporto Broadcom.	È necessario fornire un Site ID fornito da Broadcom nella richiesta di creazione dell'ambiente EVS.	01234567
Chiave di soluzione VCF	Una singola chiave di licenza VCF che sblocca le funzionalità dell'intero stack VCF, tra cui vSphere, NSX, SDDC Manager e vCenter Server.	È necessario fornire una chiave di soluzione VCF attiva valida nella richiesta di creazione dell'ambiente EVS. La chiave non può essere già utilizzata da un ambiente EVS esistente.	ABCDE-FGHIJ-KLMNO-PQRSTU-VWXYZ
Chiave di licenza vSAN	Una chiave di licenza vSAN consente di attivare e utilizzare il software vSAN all'interno di un ambiente VCF.	È necessario fornire una chiave di licenza vSAN attiva valida nella richiesta di creazione dell'ambiente EVS. La chiave non può essere già utilizzata da un ambiente EVS esistente.	ABCDE-FGHIJ-KLMNO-PQRSTU-VWXYZ

AWS informazioni sull'account e sulla regione

Componente	Description	Requisiti minimi	Valore (i) di esempio
AWS numero ID dell'account	L' AWS account consente di creare e gestire AWS risorse e accedere ai AWS servizi.	Deve avere accesso a un AWS account.	9999
AWS Regione	Un'area geografica fisica in cui sono AWS presenti più data center isolati denominati zone di disponibilità.	È necessario specificare una AWS regione in cui Amazon EVS deve essere distribuito. Per un elenco delle regioni in cui Amazon EVS è attualmente disponibile, consulta gli endpoint e le quote di Amazon Elastic VMware Service nella AWS General Reference Guide.	Stati Uniti occidentali (Oregon)

AWS Transit Gateway per la connettività dei data center locali

Componente	Description	Requisiti minimi	Valore (i) di esempio
ID gateway di transito	Un gateway di transito funge da router virtuale regionale per il flusso di traffico tra il tuo VPC e le reti locali.	È necessario utilizzare un gateway di transito per connettere un ambiente Amazon EVS alle reti locali.	Esempio TGW-0262A0E521
Metodo di connettività	Per connettere le tue reti locali a un ambiente Amazon	Determina se utilizzerai AWS Direct Connect, AWS Site-	AWS Site-to-Site VPN con AWS Direct Connect

Componente	Description	Requisiti minimi	Valore (i) di esempio
	EVS, devi utilizzare un gateway di transito con AWS Direct Connect o AWS Site-to-Site VPN.	to-Site VPN o una combinazione di entrambi. Per ulteriori informazioni sull'util izzo della Site-to-S ite VPN con Direct Connect, consulta AWS Site-to-Site VPN IP privata con AWS Direct Connect.	

VPC per ambiente Amazon EVS

Componente	Description	Requisiti minimi	Valore (i) di esempio
ID VPC	Un VPC è una rete virtuale molto simile a una rete tradizionale che gestiresti nel tuo data center.	Qualsiasi Amazon VPC può essere utilizzato per la distribuzione nell'ambi ente.	vpc-0abcdef1234567 890
Blocco CIDR VPC	In Amazon VPC, un blocco CIDR definisce l'intervallo di indirizzi IP disponibili all'inter no del tuo VPC.	Un blocco CIDR RFC 1918 con una dimensione minima di /22 netmask. Il blocco VPC CIDR deve essere di dimensioni adeguate per ospitare tutte le sottoreti e gli host EVS da implementare nel tuo VPC. Questo blocco CIDR deve essere unico in tutti gli ambienti.	10.1.0.0/20

Sottoreti VPC per ambiente EVS

Componente	Description	Requisiti minimi	Valore (i) di esempio
ID della sottorete di accesso al servizio	Una sottorete di accesso ai servizi è una sottorete VPC standard che consente l'accesso al servizio Amazon EVS. Per ulteriori informazioni, consulta the section called "Sottorete di accesso al servizio".	È possibile utilizzar e qualsiasi sottorete VPC, a condizion e che la sottorete sia di dimensioni adeguate all'interno del VPC. Suggeriam o di specificare un blocco CIDR di sottorete VPC con una netmask di /24.	subnet-abcdef12345 67890e
sottorete di accesso al servizio CIDR	un blocco CIDR di sottorete VPC è un intervallo di indirizzi IP, definito utilizzan do la notazione CIDR, che viene allocato a una sottorete specifica all'interno di un VPC.	La sottorete di accesso al servizio deve essere di dimensioni adeguate per ospitare anche le altre sottoreti e host EVS da implementare nel VPC. Suggeriam o di specificare un blocco CIDR di sottorete VPC con una netmask di /24.	10.1.0.0/24
AWS ID della zona di disponibilità all'interno della regione	Una posizione distinta all'interno di una AWS regione, progettata per essere isolata dai guasti in altre AZs regioni e costituita da uno o più data center.	È possibile specifica re la zona di disponibi lità in cui vengono distribuite le sottoreti VPC durante la creazione della sottorete. Per ulteriori informazioni, consulta Creare una sottorete	us-west-2a

Componente	Description	Requisiti minimi	Valore (i) di esempio
		nella Amazon VPC User Guide.	

Sottoreti EVS VLAN per ambiente EVS

Componente	Description	Requisiti minimi	Valore (i) di esempio
Gestione dell'host: VLAN (CIDR)	Il blocco CIDR per la sottorete VLAN di gestione dell'host. Per ulteriori informazioni, consulta the section called "Sottorete VLAN di gestione dell'host".	Deve avere una dimensione minima di /28 netmask e una dimensione massima di /24 netmask. Non deve sovrapporsi a nessun blocco CIDR esistente associato al VPC.	10.1.1.0/24
VMotion VLAN CIDR	Il blocco CIDR per la sottorete VLAN VMotion. Per ulteriori informazioni, consulta the section called "Sottorete VLAN VMotion".	Deve avere le stesse dimensioni della VLAN di gestione dell'host.	10.1.2.0/24
VSAN VLAN CIDR	Il blocco CIDR per la sottorete VLAN vSAN. Per ulteriori informazioni, consulta the section called "Sottorete VLAN vSAN".	Deve avere le stesse dimensioni della VLAN di gestione dell'host.	10.1.3.0/24
SIDRO VTEP CLAN	Il blocco CIDR per la sottorete VLAN VTEP. Per ulteriori	Deve avere le stesse dimensioni della	10.1.4.0/24

Componente	Description	Requisiti minimi	Valore (i) di esempio
	informazioni, consulta the section called "Sottorete VLAN VTEP".	VLAN di gestione dell'host.	
VLAN VTEP Edge CIDR	Il blocco CIDR per la sottorete VLAN Edge VTEP. Per ulteriori informazioni, consulta the section called "Sottorete VLAN Edge VTEP".	Deve avere una dimensione minima di /28 netmask e una dimensione massima di /24 netmask. Non deve sovrapporsi a nessun blocco CIDR esistente associato al VPC.	10.1.5.0/24
VM di gestione VLAN CIDR	Il blocco CIDR per la sottorete VLAN Management VM. Per ulteriori informazioni, consulta the section called "Sottorete VLAN di gestione (VM)".	Deve avere una dimensione minima di /28 netmask e una dimensione massima di /24 netmask. Non deve sovrapporsi a nessun blocco CIDR esistente associato al VPC.	10.1.6.0/24
CIDR VLAN in uplink HCX	Il blocco CIDR per la sottorete VLAN uplink HCX. Per ulteriori informazioni, consulta the section called "Sottorete VLAN HCX uplink".	Deve avere una dimensione minima di /28 netmask e una dimensione massima di /24 netmask. Non deve sovrapporsi a nessun blocco CIDR esistente associato al VPC.	10.1.7.0/24

Componente	Description	Requisiti minimi	Valore (i) di esempio
VLAN NSX in uplink CIDR	Il blocco CIDR per la sottorete VLAN uplink NSX. Per ulteriori informazioni, consulta the section called "Sottorete VLAN NSX uplink".	Deve avere una dimensione minima di /28 netmask e una dimensione massima di /24 netmask. Non deve sovrapporsi a nessun blocco CIDR esistente associato al VPC.	10.1.8.0/24
Espansione VLAN 1 CIDR	Blocco CIDR per la sottorete VLAN di espansione. Per ulteriori informazioni, consulta the section called "Sottorete VLAN di espansione".	Deve avere una dimensione minima di /28 netmask e una dimensione massima di /24 netmask. Non deve sovrapporsi a nessun blocco CIDR esistente associato al VPC.	10.1.9.0/24
Espansione VLAN 2 CIDR	Blocco CIDR per la sottorete VLAN di espansione. Per ulteriori informazioni, consulta the section called "Sottorete VLAN di espansione".	Deve avere una dimensione minima di /28 netmask e una dimensione massima di /24 netmask. Non deve sovrapporsi a nessun blocco CIDR esistente associato al VPC.	10.1.10.0/24

Infrastruttura DNS e NTP

Componente	Description	Requisiti minimi	Valore (i) di esempio
Indirizzo IP del server DNS primario	Il server DNS (Domain Name System) principal e utilizzato come fonte di verità per tutti i record DNS del dominio.	È possibile utilizzar e qualsiasi IPv4 indirizzo valido e non utilizzato all'interno dell'intervallo di host utilizzabili.	10.1.1.10
Indirizzo IP del server DNS secondario	Un server DNS di backup per i record DNS del dominio.	È possibile utilizzar e qualsiasi IPv4 indirizzo valido e non utilizzato all'interno dell'intervallo di host utilizzabili.	10.1.5.25
Indirizzo IP del server NTP	Un server NTP (Network Time Protocol) è un dispositivo o un'applic azione che sincroniz za gli orologi all'inter no di una rete utilizzando lo standard NTP.	Puoi utilizzare il servizio Amazon Time Sync predefinito con l'indirizzo `169.254.1 69.123` IP locale o un altro indirizzo IP del server NTP.	169.254.169.123 (servizio Amazon Time Sync)
FQDN per la distribuz ione VCF	Un nome di dominio completo (FQDN) è il nome assoluto di un dispositivo su una rete. Un FQDN è composto da un nome host e un nome di dominio.	Un FQDN può contenere solo caratteri alfanumer ici, il segno meno (-) e punti utilizzat i come delimitatori tra le etichette. Deve essere un nome di dominio completo	rispetto a local

Componente	Description	Requisiti minimi	Valore (i) di esempio
		univoco valido e non scaduto.	

Set di opzioni DHCP VPC

Componente	Description	Requisiti minimi	Valore (i) di esempio
ID del set di opzioni DHCP	Un set di opzioni DHCP è un gruppo di impostazioni di rete utilizzate dalle risorse del VPC, EC2 come le istanze, per comunicare sulla rete virtuale.	Deve contenere un minimo di 2 server DNS. È possibile utilizzare Route 53 o server DNS personalizzati. Deve contenere anche il nome di dominio DNS e un server NTP.	dopt-0a1b2c3d

EC2 coppia di key pair

Componente	Description	Requisiti minimi	Valore (i) di esempio
EC2 nome della coppia di chiavi	Una EC2 key pair è un insieme di credenziali di sicurezza utilizzate per connettersi in modo sicuro a un'istanza Amazon EC2 .	Il nome della coppia di chiavi deve essere univoco.	`my-ec2-key-pair`

Tabelle di routing VPC

Componente	Description	Requisiti minimi	Valore (i) di esempio
ID della tabella di rotta principale	In Amazon VPC, la tabella di routing principale è la tabella di routing predefinita creata automaticamente con il VPC e regola il traffico per tutte le sottoreti VPC che non sono associate esplicitamente a una tabella di routing diversa. Le sottoreti VLAN EVS sono associate implicitamente alla tabella di routing principale del tuo VPC quando Amazon EVS le crea.	Deve essere configurato per abilitare la connettività a servizi dipendenti come DNS o sistemi locali affinché la distribuzione dell'ambiente abbia successo.	rtb-0123456789abcdef0

Lista di controllo degli accessi di rete (ACL)

Componente	Description	Requisiti minimi	Valore (i) di esempio
ID ACL di rete	Una lista di controllo dell'accesso alla rete (ACL) consente o nega il traffico in entrata o in uscita a livello di sottorete.	Deve consentire ad Amazon EVS di comunicare con: • Server DNS sulla TCP/UDP porta 53. • Sottorete VLAN di gestione dell'host	acl-0f62c640e793a38a3

Componente	Description	Requisiti minimi	Valore (i) di esempio
		tramite HTTPS e SSH. • Sottorete VLAN VM di gestione tramite HTTPS e SSH.	

Record DNS per componenti VCF

Componente	Description	Requisiti minimi	Esempio di indirizzo IP	Esempio di hostname
Host ESX 1	Indirizzo IP e nome host definiti nel record A e nel record PTR per l'host ESX 1.	Amazon EVS richiede una zona di ricerca diretta DNS con record A e una zona di ricerca inversa con record PTR creati per ogni host ESX in ogni implementazione EVS.	10.1.0.10	esxi01
host ESX 2	Indirizzo IP e nome host definiti nel record A e nel record PTR per l'host ESX 2.	Amazon EVS richiede una zona di ricerca diretta DNS con record A e una zona di ricerca inversa con record PTR creati per ogni host ESX in ogni	10.1.0.11	esxi02

Componente	Description	Requisiti minimi	Esempio di indirizzo IP	Esempio di hostname
		implementazione EVS.		
host ESX 3	Indirizzo IP e nome host definiti nel record A e nel record PTR per l'host ESX 3.	Amazon EVS richiede una zona di ricerca diretta DNS con record A e una zona di ricerca inversa con record PTR creati per ogni host ESX in ogni implementazione EVS.	10.1.0.12	esxi03
host ESX 4	Indirizzo IP e nome host definiti nel record A e nel record PTR per l'host ESX 4.	Amazon EVS richiede una zona di ricerca diretta DNS con record A e una zona di ricerca inversa con record PTR creati per ogni host ESX in ogni implementazione EVS.	10.1.0.13	esxi04

Componente	Description	Requisiti minimi	Esempio di indirizzo IP	Esempio di hostname
Appliance vCenter Server	Indirizzo IP e nome host definiti nel record A e nel record PTR per l'appliance vCenter Server.	Amazon EVS richiede una zona di ricerca diretta DNS con record A e una zona di ricerca inversa con record PTR creati per ogni appliance di gestione VCF in ogni implementazione EVS.	10.1.5.10	vc01
Cluster NSX Manager	Indirizzo IP e nome host definiti nel record A e nel record PTR per il cluster NSX Manager.	Amazon EVS richiede una zona di ricerca diretta DNS con record A e una zona di ricerca inversa con record PTR creati per ogni appliance di gestione VCF in ogni implementazione EVS.	10.1.5.11	nsx

Componente	Description	Requisiti minimi	Esempio di indirizzo IP	Esempio di hostname
dispositivo SDDC Manager	Indirizzo IP e nome host definiti nel record A e nel record PTR per l'appliance SDDC Manager.	Amazon EVS richiede una zona di ricerca diretta DNS con record A e una zona di ricerca inversa con record PTR creati per ogni appliance di gestione VCF in ogni implement azione EVS.	10.1.5.12	sddcm01
Dispositivo Cloud Builder	Indirizzo IP e nome host definiti nel record A e nel record PTR per l'applian ce Cloud Builder.	Amazon EVS richiede una zona di ricerca diretta DNS con record A e una zona di ricerca inversa con record PTR creati per ogni appliance di gestione VCF in ogni implement azione EVS.	10.1.5.13	cb01

Componente	Description	Requisiti minimi	Esempio di indirizzo IP	Esempio di hostname
Dispositivo NSX Edge 1	Indirizzo IP e nome host definiti nel record A e nel record PTR per l'appliance NSX Edge 1.	Amazon EVS richiede una zona di ricerca diretta DNS con record A e una zona di ricerca inversa con record PTR creati per ogni appliance di gestione VCF in ogni implementazione EVS.	10.1.5.14	spigolo 01
Dispositivo NSX Edge 2	Indirizzo IP e nome host definiti nel record A e nel record PTR per l'appliance NSX Edge 2.	Amazon EVS richiede una zona di ricerca diretta DNS con record A e una zona di ricerca inversa con record PTR creati per ogni appliance di gestione VCF in ogni implementazione EVS.	10.1.5.15	spigolo 02

Componente	Description	Requisiti minimi	Esempio di indirizzo IP	Esempio di hostname
Dispositivo NSX Manager 1	Indirizzo IP e nome host definiti nel record A e nel record PTR per l'appliance NSX Manager 1.	Amazon EVS richiede una zona di ricerca diretta DNS con record A e una zona di ricerca inversa con record PTR creati per ogni appliance di gestione VCF in ogni implementazione EVS.	10.1.5.16	nsx01
Dispositivo NSX Manager 2	Indirizzo IP e nome host definiti nel record A e nel record PTR per l'appliance NSX Manager 2.	Amazon EVS richiede una zona di ricerca diretta DNS con record A e una zona di ricerca inversa con record PTR creati per ogni appliance di gestione VCF in ogni implementazione EVS.	10.1.5.17	NSX 02

Componente	Description	Requisiti minimi	Esempio di indirizzo IP	Esempio di hostname
Dispositivo NSX Manager 3	Indirizzo IP e nome host definiti nel record A e nel record PTR per l'appliance NSX Manager 3.	Amazon EVS richiede una zona di ricerca diretta DNS con record A e una zona di ricerca inversa con record PTR creati per ogni appliance di gestione VCF in ogni implementazione EVS.	10.1.5.18	NSX 03

Infrastruttura VPC Route Server

Componente	Description	Requisiti minimi	Valore o valori di esempio
ID del server di routing	Amazon EVS utilizza Amazon VPC Route Server per abilitare il routing dinamico basato su BGP verso la tua rete overlay VPC.	È necessario specificare un server di routing che condivida le rotte verso almeno due endpoint del server di routing nella sottorete di accesso al servizio. L'ASN peer configurato sul route server e il peer NSX Edge devono corrispondere e gli indirizzi IP del peer devono essere univoci.	rs-0a1b2c3d4e5f67890

Componente	Description	Requisiti minimi	Valore o valori di esempio
associazione di server di routing	La connessione tra un server di routing e un VPC.	Il server di routing deve essere associato al tuo VPC.	{ "RouteServerAssociation": { "RouteServerId": "rs-0a1b2c3d4e5f67890", "VpcId": "vpc-1", "State": "associating" } }
ASN BGP del lato VPC Route Server (ASN lato Amazon)	L'ASN lato Amazon rappresenta il AWS lato della sessione BGP tra il server di routing VPC e il peer NSX Edge. È necessario specificare questo ASN BGP durante la creazione del server di routing. Per ulteriori informazioni, consulta Creare un server di routing nella Amazon VPC User Guide.	Questo valore deve essere univoco e compreso tra 1 e 4294967295. AWS consiglia di utilizzare un ASN privato nell'intervallo 64512—65534 (ASN a 16 bit) o 4200000000—4294967294 (ASN a 32 bit).	65001

Componente	Description	Requisiti minimi	Valore o valori di esempio
ID dell'endpoint 1 del server di routing	Un endpoint del server di routing è un componente AWS gestito all'interno di una sottorete che facilita le connessioni BGP (Border Gateway Protocol) tra il server di routing e i peer BGP.	È necessario distribuire l'endpoint del server di routing nella sottorete di accesso al servizio.	rse-0123456789abcdef0
server di routing per 1 ID	Il route server peer è una sessione di peering BGP tra un endpoint del server di routing e il dispositivo distribuito in (NSX Edge). AWS	Il valore ASN peer specificato nel route server peer deve corrispondere al valore ASN peer utilizzato per il gateway NSX Edge Tier-0.	rsp-0123456789abcdef0
server di routing per 1 indirizzo IP (lato EVS NSX Edge 1)	L'indirizzo IP del server di routing peer (). `PeerAddress`	È necessario utilizzare un indirizzo IP univoco non utilizzato dalla VLAN di uplink NSX. Amazon EVS applicherà questo indirizzo IP a NSX Edge 1 come parte della distribuzione e del peer con l'endpoint peer del server di routing.	10.1.7.10

Componente	Description	Requisiti minimi	Valore o valori di esempio
indirizzo ENI del server di routing per 1 endpoint	L'indirizzo IP ENI dell'endpoint del server di routing peer (). `EndpointEniAddress`	Generato automatic amente dal server di routing alla creazione del peer.	10.1.7.11
ID dell'endpoint 2 del server di routing	Un endpoint del server di routing è un componente AWS gestito all'interno di una sottorete che facilita le connessioni BGP (Border Gateway Protocol) tra il server di routing e i peer BGP.	È necessario distribui re l'endpoint del server di routing nella sottorete di accesso al servizio.	rse-fedcba9876543210f
ID del server di routing peer 2 (lato EVS NSX Edge 2)	Il route server peer è una sessione di peering BGP tra un endpoint del server di routing e il dispositi vo distribuito in (NSX Edge). AWS	Il valore ASN peer specificato nel route server peer deve corrispondere al valore ASN peer utilizzato per il gateway NSX Edge Tier-0.	rsp-fedcba9876543210f

Componente	Description	Requisiti minimi	Valore o valori di esempio
indirizzo IP peer 2 del server di routing	L'indirizzo IP del server di routing peer ()`PeerAddress` .	È necessario utilizzare un indirizzo IP univoco dalla VLAN di uplink NSX. Amazon EVS applicherà questo indirizzo IP a NSX Edge 2 come parte della distribuzione e del peer con l'endpoint peer del server di routing.	10.1.7.200
indirizzo ENI del server di routing peer 2 endpoint	L'indirizzo IP ENI dell'endpoint del server di routing peer (). `EndpointEniAddress`	Generato automaticamente dal server di routing alla creazione del peer.	10.1.7.201
propagazione del server di routing	La propagazione del server di routing installa le rotte nel FIB nella tabella di route specificata.	È necessario specificare la tabella di routing associata alla sottorete di accesso al servizio. Al momento Amazon EVS supporta solo il IPv4 networking.	`{ "RouteServerEndpoint": { "RouteServerId": "rs-1", "RouteServerEndpointId": "rse-1", "VpcId": "vpc-1", "SubnetId": "subnet-1", "State": "pending" } }`

Componente	Description	Requisiti minimi	Valore o valori di esempio
ASN BGP del lato peer di NSX	ASN BGP per il lato NSX della connessione.	Suggerisci di utilizzare l'ASN 65000 predefinito di NSX	65000

Risorse di accesso a Internet HCX (opzionali)

Componente	Description	Requisiti minimi	Valore (i) di esempio
ID IPAM	Amazon VPC IP Address Manager (IPAM) utilizzato per gestire gli indirizzi IP per l'accesso a Internet HCX.	Deve essere configurato per fornire indirizzi pubblici. IPv4 Richiesto solo per la configurazione dell'accesso a Internet HCX.	ipam-0123456789abcdef0
ID del pool IPAM	Un pool IPv4 IPAM pubblico di proprietà di Amazon che fornisce indirizzi per i componenti HCX.	Deve essere configurato come pool pubblico. IPv4 Richiesto solo per la configurazione dell'accesso a Internet HCX.	ipam-pool-0123456789abcdef0
blocco CIDR VLAN pubblico HCX	Un blocco IPv4 CIDR pubblico secondario allocato dal pool IPAM per la sottorete VLAN pubblica HCX.	Deve avere una netmask /28 ed essere allocato dal pool pubblico IPAM di proprietà di Amazon. Richiesto solo per la configurazione dell'accesso a Internet HCX.	18.97.137.0/28

Componente	Description	Requisiti minimi	Valore (i) di esempio
Indirizzi IP elastici	Indirizzi IP elastici sequenziali allocati dal pool IPAM per i componenti HCX.	Almeno 3 EIPs dallo stesso pool IPAM per HCX Manager, HCX Interconnect Appliance (HCX-IX) e HCX Network Extension (HCX-NE). Richiesto solo per la configurazione dell'accesso a Internet HCX.	eipalloc-0123456789abcdef0, eipalloc-0123456789abcdef1, eipalloc-0123456789abcdef2

Guida introduttiva ad Amazon Elastic VMware Service

Usa questa guida per iniziare a usare Amazon Elastic VMware Service (Amazon EVS). Imparerai come creare un ambiente Amazon EVS con host all'interno del tuo Amazon Virtual Private Cloud (VPC).

Al termine, avrai a disposizione un ambiente Amazon EVS che potrai utilizzare per migrare i tuoi carichi di lavoro VMware basati su vSphere verso. Cloud AWS

Important

Per iniziare nel modo più semplice e veloce possibile, questo argomento include i passaggi per creare un VPC e specifica i requisiti minimi per la configurazione del server DNS e la creazione dell'ambiente Amazon EVS. Prima di creare queste risorse, ti consigliamo di pianificare lo spazio degli indirizzi IP e la configurazione dei record DNS in modo da soddisfare i tuoi requisiti. È inoltre necessario acquisire familiarità con i requisiti di VCF 5.2.x. Consulta le note di rilascio di VCF 5.2.x per le informazioni di rilascio pertinenti.

Important

Per informazioni sulle versioni VCF fornite da Amazon EVS, consulta. the section called "Versioni VCF e istanze EC2"

Argomenti

- Verifica la creazione dell'ambiente Amazon EVS
- Associa esplicitamente le sottoreti VLAN di Amazon EVS a una tabella di routing VPC
- Recupera le credenziali VCF e accedi ai dispositivi di gestione VCF
- Eliminazione
- Fasi successive

Prerequisiti

Prima di iniziare, devi completare le attività prerequisite di Amazon EVS. Per ulteriori informazioni, consulta Configurazione di Amazon Elastic VMware Service.

Crea un VPC con sottoreti e tabelle di routing

> **Note**
>
> Il VPC, le sottoreti e l'ambiente Amazon EVS devono essere creati tutti nello stesso account. Amazon EVS non supporta la condivisione tra account di sottoreti VPC o ambienti Amazon EVS.

Example

Amazon VPC console

1. Apri la Amazon VPC console.
2. Nella scheda VPC, scegli Create VPC (Crea modulo VPC).
3. Per Risorse da creare, scegli VPC e altro.
4. Per creare tag dei nomi per le risorse VPC, tieni selezionata Generazione automatica dei tag dei nomi altrimenti deselezionala per scegliere autonomamente tag dei nomi per le risorse VPC.
5. Per il blocco IPv4 CIDR, inserisci un blocco CIDR. IPv4 Un VPC deve avere un blocco IPv4 CIDR. Assicurati di creare un VPC di dimensioni adeguate per ospitare le sottoreti Amazon EVS. Per ulteriori informazioni, consulta the section called “Considerazioni sulla rete Amazon EVS”.

> **Note**
>
> Amazon EVS non supporta IPv6 al momento.

6. Mantieni Tenancy come. `Default` Con questa opzione selezionata, le istanze EC2 avviate in questo VPC utilizzeranno l'attributo tenancy specificato al momento dell'avvio delle istanze. Amazon EVS lancia istanze EC2 bare metal per tuo conto.
7. Per Numero di zone di disponibilità () AZs, scegli 1.

> **Note**
>
> Al momento Amazon EVS supporta solo implementazioni Single-AZ.

8. Espandi Personalizza AZs e scegli la AZ per le tue sottoreti.

> **Note**
>
> È necessario eseguire la distribuzione in una AWS regione in cui è supportato Amazon EVS. Per ulteriori informazioni sulla disponibilità della regione Amazon EVS, consulta gli endpoint e le quote di Amazon Elastic VMware Service nella Guida di riferimento AWS generale.

9. (Facoltativo) Se hai bisogno di connettività Internet, per Numero di sottoreti pubbliche, scegli 1.
10. Per Numero di sottoreti private, scegli 1. Questa sottorete privata verrà utilizzata come sottorete di accesso al servizio fornita ad Amazon EVS durante la fase di creazione dell'ambiente. Per ulteriori informazioni, consulta the section called "Sottorete di accesso al servizio".
11. Per scegliere gli intervalli di indirizzi IP delle sottoreti, espandi Personalizza i blocchi CIDR delle sottoreti.

> **Note**
>
> Le sottoreti VLAN di Amazon EVS dovranno inoltre essere create da questo spazio CIDR VPC. Assicurati di lasciare spazio sufficiente nel blocco CIDR VPC per le sottoreti VLAN richieste dal servizio. Per ulteriori informazioni, consulta the section called "Considerazioni sulla rete Amazon EVS"

12. (Facoltativo) Per concedere l'accesso a Internet alle risorse, IPv4 per i gateway NAT, scegliete In 1 AZ. Tieni presente che esiste un costo associato ai gateway NAT. Per ulteriori informazioni, consulta Prezzi per i gateway NAT.

> **Note**
>
> Amazon EVS richiede l'uso di un gateway NAT per abilitare la connettività Internet in uscita.

13. Per VPC endpoints (Endpoint VPC), scegli None (Nessuno).

> **Note**
>
> Amazon EVS non supporta gli endpoint VPC gateway Amazon S3 per il momento. Per abilitare la Amazon S3 connettività, è necessario configurare un'interfaccia VPC endpoint utilizzando for. AWS PrivateLink Amazon S3 Per ulteriori informazioni, consulta AWS PrivateLink la Guida per Amazon S3 l'utente di Amazon Simple Storage Service.

14. Per le opzioni DNS, mantieni selezionate le impostazioni predefinite. Amazon EVS richiede che il tuo VPC disponga di funzionalità di risoluzione DNS per tutti i componenti VCF.

15. (Facoltativo) Per aggiungere un tag al VPC, espandi Altri tag, scegli Aggiungi nuovo tag e immetti una chiave e un valore di tag.

16. Seleziona Crea VPC.

> **Note**
>
> Durante la creazione di un VPC, crea Amazon VPC automaticamente una tabella di routing principale e associa implicitamente le sottoreti ad essa per impostazione predefinita.

AWS CLI

1. Aprire una sessione terminale.
2. Crea un VPC con una sottorete privata e una sottorete pubblica opzionale in un'unica zona di disponibilità.

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

VPC_ID=$ (aws ec2 describe-vpcs\ --filters name=tag:Nome, valori=EVS-VPC\ --query 'Vpcs [0]. VpcId'\ --testo in uscita) ---

3. Abilita i nomi host DNS e il supporto DNS.

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

4. Crea una sottorete privata nel VPC.

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

5. Memorizza l'ID di sottorete privato per utilizzarlo nei comandi successivi.

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

6. (Facoltativo) Crea una sottorete pubblica se è necessaria la connettività Internet.

```
aws ec2 create-subnet \
  --vpc-id $VPC_ID \
  --cidr-block 10.0.0.0/24 \
```

```
  --availability-zone us-west-2a \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=evs-public-
subnet}]'
```

7. (Facoltativo) Memorizza l'ID pubblico della sottorete da utilizzare nei comandi successivi.

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

8. (Facoltativo) Crea e collega un gateway Internet se viene creata la sottorete pubblica.

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

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

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

9. (Facoltativo) Crea un gateway NAT se è necessaria la connettività Internet.

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

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

aws ec2 create-nat-gateway \
  --subnet-id $PUBLIC_SUBNET_ID \
  --allocation-id $EIP_ID \
  --tag-specifications 'ResourceType=natgateway,Tags=[{Key=Name,Value=evs-nat}]'
```

10. Crea e configura le tabelle di routing necessarie.

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

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

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

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

11. Aggiungi i percorsi necessari alle tabelle delle rotte.

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

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

12. Associa le tabelle delle rotte alle tue sottoreti.

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

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

```
  --subnet-id $PUBLIC_SUBNET_ID
```

> **Note**
>
> Durante la creazione di un VPC, crea Amazon VPC automaticamente una tabella di routing principale e associa implicitamente le sottoreti ad essa per impostazione predefinita.

Scegli la tua opzione di connettività HCX

Seleziona un'opzione di connettività per il tuo ambiente Amazon EVS:

- Connettività privata: fornisce percorsi di rete ad alte prestazioni per HCX, ottimizzando l'affidabilità e la coerenza. Richiede l'uso di AWS Direct Connect o Site-to-Site VPN per la connettività di rete esterna.
- Connettività Internet: utilizza la rete Internet pubblica per stabilire un percorso di migrazione flessibile e rapido da configurare. Richiede l'uso di VPC IP Address Manager (IPAM) e indirizzi IP elastici.

Per un'analisi dettagliata, vedere. the section called “Opzioni di connettività HCX”

Scegli la tua opzione:

- Opzione A: Solo connettività privata → Continua athe section called “Configurare la tabella di routing principale del VPC”.
- Opzione B: connettività Internet → Continua athe section called “Configurazione della connettività Internet HCX”.

Configurazione della connettività Internet HCX

> **Note**
>
> Salta questa sezione se hai scelto la connettività privata HCX e continua a farlo. the section called “Configurare la tabella di routing principale del VPC”

Per abilitare la connettività Internet HCX per Amazon EVS, devi:

- Assicurati che la tua quota IPAM (VPC IP Address Manager) per la lunghezza della netmask del blocco IPv4 CIDR pubblico contiguo fornita da Amazon sia /28 o superiore.

  > **Important**
  >
  > L'uso di qualsiasi blocco IPv4 CIDR pubblico contiguo fornito da Amazon con una lunghezza della maschera di rete inferiore a /28 comporterà problemi di connettività HCX. Per ulteriori informazioni sull'aumento delle quote IPAM, consulta Quote per il tuo IPAM.

- Crea un IPAM e un pool IPv4 IPAM pubblico con un CIDR con una lunghezza minima della maschera di rete di /28.
- Alloca almeno due indirizzi IP elastici (EIPs) dal pool IPAM per i dispositivi HCX Manager e HCX Interconnect (HCX-IX). Assegna un indirizzo IP elastico aggiuntivo per ogni appliance di rete HCX da distribuire.
- Aggiungi il blocco IPv4 CIDR pubblico come CIDR aggiuntivo al tuo VPC.

Per ulteriori informazioni sulla gestione della connettività Internet HCX dopo la creazione dell'ambiente, consulta. the section called "Connettività pubblica HCX"

Creare un IPAM

Segui questi passaggi per creare un IPAM.

> **Note**
>
> Puoi utilizzare IPAM Free Tier per creare risorse IPAM da utilizzare con Amazon EVS. Sebbene IPAM stesso sia gratuito con Free Tier, sei responsabile dei costi di altri AWS servizi utilizzati in combinazione con IPAM, come i gateway NAT e tutti IPv4 gli indirizzi pubblici che utilizzi che superano il limite del piano gratuito. Per ulteriori informazioni sui prezzi IPAM, consulta la pagina dei prezzi.Amazon VPC

> **Note**
>
> Al momento Amazon EVS non supporta l'indirizzo GUA (IPv6 Global Unicast CIDRs Address) privato.

Crea un pool IPAM pubblico IPv4

Segui questi passaggi per creare un IPv4 pool pubblico.

IPAM console

1. Apri la console IPAM.
2. Nel pannello di navigazione, seleziona Pool.
3. Scegli l'ambito Public (Pubblico). Per ulteriori informazioni sugli ambiti, consulta Come funziona IPAM.
4. Scegli Crea pool.
5. (Facoltativo) Aggiungi un Name tag (Tag nome) e una Description (Descrizione) per il pool.
6. In Famiglia di indirizzi, scegli. IPv4
7. In Resource planning (Pianificazione delle risorse), lascia selezionato Plan IP space within the scope (Pianifica spazio IP nell'ambito).
8. In Locale (Località), scegli la località per il pool. La lingua è la AWS regione in cui desideri che questo pool IPAM sia disponibile per le allocazioni. La locale scelta deve corrispondere alla AWS regione in cui è distribuito il VPC.
9. In Service (Servizio), scegli EC2 (EIP/VPC). Questo pubblicizzerà i CIDR allocati da questo pool per il servizio Amazon EC2 (per indirizzi IP elastici).
10. In Origine IP pubblica, scegli Di proprietà di Amazon.
11. Sotto CIDRs alla disposizione, scegli Aggiungi CIDR pubblico di proprietà di Amazon.
12. In Netmask, scegli la lunghezza della netmask CIDR. /28 è la lunghezza minima richiesta per la netmask.
13. Scegli Crea pool.

AWS CLI

1. Apri una sessione terminale.

2. Ottieni l'ID dell'ambito pubblico dal tuo IPAM.

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

3. Crea un pool IPAM nell'ambito pubblico.

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

4. Memorizza l'ID del pool per utilizzarlo nei comandi successivi.

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

5. Esegui il provisioning di un blocco CIDR dal pool con una lunghezza minima della netmask di /28.

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

Alloca gli indirizzi IP elastici dal pool IPAM

Segui questi passaggi per allocare gli indirizzi IP elastici (EIPs) dal pool IPAM per le appliance HCX Service Mesh.

Amazon VPC console

1. Apri la Console Amazon VPC.
2. Nel pannello di navigazione, scegli Elastic. IPs
3. Scegli Alloca indirizzo IP elastico.
4. Seleziona Alloca utilizzando un pool IPv4 IPAM.
5. Seleziona il IPv4 pool pubblico di proprietà di Amazon che hai configurato in precedenza.
6. In Metodo Allocate IPAM, scegli Inserisci manualmente l'indirizzo all'interno del pool IPAM.

> **Important**
>
> Non è possibile associare i primi due EIPs o gli ultimi EIP dal blocco CIDR IPAM pubblico alla sottorete VLAN. Questi EIPs sono riservati come indirizzi di rete, gateway predefiniti e indirizzi di trasmissione. Amazon EVS genera un errore di convalida se tenti di EIPs associarli alla sottorete VLAN.

> **Important**
>
> Inserisci manualmente gli indirizzi all'interno del pool IPAM per garantire EIPs che le riserve Amazon EVS non vengano allocate. Se consenti a IPAM di scegliere l'EIP, IPAM può allocare un EIP riservato da Amazon EVS, causando errori durante l'associazione EIP alla sottorete VLAN.

7. Specificare l'EIP da allocare dal pool IPAM.
8. Scegli Alloca.
9. Ripetere questa procedura per allocare il resto EIPs necessario. È necessario allocarne almeno due EIPs dal pool IPAM per i dispositivi HCX Manager e HCX Interconnect (HCX-IX). Assegna un EIP aggiuntivo per ogni appliance di rete HCX da distribuire.

AWS CLI

1. Aprire una sessione terminale.
2. Ottieni l'ID del pool IPAM che hai creato in precedenza.

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

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

3. Alloca gli indirizzi IP elastici dal pool IPAM. È necessario allocarne almeno due EIPs dal pool IPAM per le appliance HCX Manager e HCX Interconnect (HCX-IX). Assegna un EIP aggiuntivo per ogni appliance di rete HCX da distribuire.

> **Important**
>
> Non è possibile associare i primi due EIPs o gli ultimi EIP del blocco CIDR IPAM pubblico a una sottorete VLAN. Questi EIPs sono riservati come indirizzi di rete, gateway predefiniti e indirizzi di trasmissione. Amazon EVS genera un errore di convalida se tenti di EIPs associarli alla sottorete VLAN.

> **Important**
>
> Inserisci manualmente gli indirizzi all'interno del pool IPAM per garantire EIPs che le riserve Amazon EVS non vengano allocate. Se consenti a IPAM di scegliere l'EIP, IPAM può allocare un EIP riservato da Amazon EVS, causando errori durante l'associazione EIP alla sottorete VLAN.

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

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

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

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

Aggiungi il blocco IPv4 CIDR pubblico dal pool IPAM al VPC per la connettività Internet HCX

Per abilitare la connettività Internet HCX, devi aggiungere il blocco IPv4 CIDR pubblico dal pool IPAM al tuo VPC come CIDR aggiuntivo. Amazon EVS utilizza questo blocco CIDR per connettere VMware HCX alla tua rete. Segui questi passaggi per aggiungere il blocco CIDR al tuo VPC.

> **Important**
>
> Devi inserire manualmente il blocco IPv4 CIDR che aggiungi al tuo VPC. Al momento Amazon EVS non supporta l'uso di un blocco CIDR allocato su IPAM. L'uso di un blocco CIDR allocato su IPAM può causare un errore di associazione EIP.

Amazon VPC console

1. Apri la Console Amazon VPC.
2. Nel riquadro di navigazione, scegli Your. VPCs
3. Seleziona il VPC che hai creato in precedenza e scegli Azioni, Modifica. CIDRs
4. Scegli Aggiungi nuovo IPV4 CIDR.
5. Seleziona l'immissione manuale IPV4 CIDR.
6. Specificate il blocco CIDR dal pool IPAM pubblico creato in precedenza.

AWS CLI

1. Aprire una sessione terminale.
2. Ottieni l'ID del pool IPAM e il blocco CIDR fornito.

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

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

3. Aggiungi il blocco CIDR al tuo VPC.

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

Configurare la tabella di routing principale del VPC

Le sottoreti VLAN di Amazon EVS sono associate implicitamente alla tabella di routing principale del VPC. Per abilitare la connettività a servizi dipendenti come DNS o sistemi locali per una corretta implementazione dell'ambiente, è necessario configurare la tabella di routing principale per consentire il traffico verso questi sistemi. La tabella di routing principale deve includere una route per il CIDR del VPC. L'uso della tabella di routing principale è richiesto solo per la distribuzione iniziale dell'ambiente Amazon EVS. Dopo la distribuzione dell'ambiente, puoi configurare l'ambiente per utilizzare una tabella di routing personalizzata. Per ulteriori informazioni, consulta the section called "Configura una tabella di routing personalizzata".

Dopo la distribuzione dell'ambiente, devi associare esplicitamente ciascuna delle sottoreti VLAN di Amazon EVS a una tabella di routing nel tuo VPC. La connettività NSX fallisce se le sottoreti VLAN non sono associate esplicitamente a una tabella di routing VPC. Si consiglia vivamente di associare esplicitamente le sottoreti a una tabella di routing personalizzata dopo la distribuzione dell'ambiente. Per ulteriori informazioni, consulta the section called "Configurare la tabella di routing principale del VPC".

> **Important**
>
> Amazon EVS supporta l'uso di una tabella di routing personalizzata solo dopo la creazione dell'ambiente Amazon EVS. Le tabelle di routing personalizzate non devono essere utilizzate durante la creazione dell'ambiente Amazon EVS, poiché ciò potrebbe causare problemi di connettività.

Configurazione dei server DNS e NTP utilizzando il set di opzioni VPC DHCP

Important

L'implementazione del tuo ambiente fallisce se non soddisfi questi requisiti di Amazon EVS:

- Includi un indirizzo IP del server DNS primario e un indirizzo IP del server DNS secondario nel set di opzioni DHCP.
- Includi una zona di ricerca diretta DNS con record A per ogni appliance di gestione VCF e host Amazon EVS nella tua distribuzione.
- Includi una zona di ricerca inversa DNS con record PTR per ogni appliance di gestione VCF e host Amazon EVS nella tua distribuzione.
- Configura la tabella di routing principale del VPC per assicurarti che esista un percorso verso i tuoi server DNS.
- Assicurati che la registrazione del nome di dominio sia valida e non sia scaduta e che non esistano nomi host o indirizzi IP duplicati.
- Configura i gruppi di sicurezza e le liste di controllo degli accessi alla rete (ACLs) per consentire ad Amazon EVS di comunicare con:
  - Server DNS sulla TCP/UDP porta 53.
  - Sottorete VLAN di gestione dell'host tramite HTTPS e SSH.
  - Sottorete VLAN di gestione tramite HTTPS e SSH.

Amazon EVS utilizza il set di opzioni DHCP del tuo VPC per recuperare quanto segue:

- Server DNS (Domain Name System) per la risoluzione degli indirizzi IP dell'host.
- Nomi di dominio per la risoluzione DNS.
- Server Network Time Protocol (NTP) per la sincronizzazione dell'ora.

È possibile creare un set di opzioni DHCP utilizzando la Amazon VPC console o. AWS CLI Per ulteriori informazioni, consulta Creare un set di opzioni DHCP nella Guida per l' Amazon VPC utente.

Configurare i server DNS

La configurazione DNS consente la risoluzione dei nomi host nel tuo ambiente Amazon EVS. Per implementare correttamente un ambiente Amazon EVS, il set di opzioni DHCP del tuo VPC deve avere le seguenti impostazioni DNS:

- Un indirizzo IP del server DNS primario e un indirizzo IP del server DNS secondario nel set di opzioni DHCP.
- Una zona di ricerca diretta DNS con record A per ogni appliance di gestione VCF e host Amazon EVS nella tua distribuzione.
- Una zona di ricerca inversa con record PTR per ogni appliance di gestione VCF e host Amazon EVS nella tua distribuzione. Per la configurazione NTP, puoi utilizzare l'indirizzo `169.254.169.123` Amazon NTP predefinito o un altro IPv4 indirizzo che preferisci.

Per ulteriori informazioni sulla configurazione dei server DNS in un set di opzioni DHCP, consulta Creare un set di opzioni DHCP.

Configura DNS per la connettività locale

Per la connettività locale, consigliamo l'uso di zone ospitate private Route 53 con resolver in ingresso. Questa configurazione consente la risoluzione DNS ibrida, in cui è possibile utilizzare Route 53 per il DNS interno all'interno del VPC e integrarlo con l'infrastruttura DNS locale esistente. Ciò consente alle risorse all'interno del tuo VPC di risolvere i nomi di dominio ospitati sulla tua rete locale e viceversa, senza richiedere configurazioni complesse. Se necessario, puoi anche utilizzare il tuo server DNS con i resolver in uscita Route 53. Per i passaggi di configurazione, consulta Creazione di una zona ospitata privata e Inoltro di query DNS in entrata al tuo VPC nella Amazon Route 53 Developer Guide.

> **Note**
>
> L'utilizzo sia di Route 53 che di un server DNS (Domain Name System) personalizzato nel set di opzioni DHCP può causare un comportamento imprevisto.

> **Note**
>
> Se utilizzi nomi di dominio DNS personalizzati definiti in una zona ospitata privata in Route 53 o utilizzi DNS privato con interfaccia VPC endpoints (AWS PrivateLink), devi impostare

entrambi gli attributi e su. `enableDnsHostnames` `enableDnsSupport` `true` Per ulteriori informazioni, consulta Attributi DNS per il tuo VPC.

Risolvi i problemi di raggiungibilità del DNS

Amazon EVS richiede una connessione persistente a SDDC Manager e ai server DNS nel set di opzioni DHCP del tuo VPC per raggiungere i record DNS. Se la connessione persistente a SDDC Manager non è più disponibile, Amazon EVS non sarà più in grado di convalidare lo stato dell'ambiente e potresti perdere l'accesso all'ambiente. Per i passaggi da seguire per risolvere questo problema, consulta. the section called "Controllo di raggiungibilità non riuscito"

Configurare i server NTP

I server NTP forniscono il tempo alla rete. Un riferimento temporale coerente e preciso sull'istanza Amazon EC2 è fondamentale per molte attività e processi dell'ambiente VCF. La sincronizzazione dell'ora è essenziale per:

- Registrazione e controllo del sistema
- Operazioni di sicurezza
- Gestione distribuita del sistema
- Risoluzione dei problemi

Puoi inserire gli IPv4 indirizzi di un massimo di quattro server NTP nel set di opzioni DHCP del tuo VPC. Puoi specificare Amazon Time Sync Service all' IPv4 indirizzo`169.254.169.123`. Per impostazione predefinita, le istanze Amazon EC2 distribuite da Amazon EVS utilizzano Amazon Time Sync Service all'indirizzo. IPv4 `169.254.169.123`

Per ulteriori informazioni sui server NTP, consulta RFC 2123. Per ulteriori informazioni su Amazon Time Sync Service, consulta Sincronizzazione di precisione dell'orologio e dell'ora nell'istanza EC2 e Configurazione di NTP sugli host VMware Cloud Foundation nella documentazione di Cloud Foundation. VMware

Per configurare le impostazioni NTP

1. Scegli la tua fonte NTP:
   - Servizio Amazon Time Sync (consigliato)

- Server NTP personalizzati

2. Aggiungi server NTP al set di opzioni DHCP. Per ulteriori informazioni, consulta Creare un set di opzioni DHCP nella Amazon VPC User Guide.
3. Verifica la sincronizzazione dell'ora. Per ulteriori informazioni sulla configurazione del set di opzioni DHCP, vedere. the section called "Configura il set di opzioni DHCP del tuo VPC"

Configurare la connettività di rete locale (opzionale)

È possibile configurare la connettività tra il data center locale e l' AWS infrastruttura utilizzando Direct Connect un gateway di transito associato o utilizzando un allegato AWS Site-to-Site VPN a un gateway di transito.

Per abilitare la connettività ai sistemi locali per una corretta implementazione dell'ambiente, è necessario configurare la tabella di routing principale del VPC per consentire il traffico verso questi sistemi. Per ulteriori informazioni, consulta the section called "Configurare la tabella di routing principale del VPC".

Dopo aver creato l'ambiente Amazon EVS, devi aggiornare le tabelle di routing del gateway di transito con il CIDRs VPC creato all'interno dell'ambiente Amazon EVS. Per ulteriori informazioni, consulta the section called "Configurazione delle tabelle di routing del gateway di transito e dei prefissi Direct Connect per la connettività locale (opzionale)".

Per ulteriori informazioni sulla configurazione di una Direct Connect connessione, consulta Gateway and Transit Direct Connect Gateway Associations. Per ulteriori informazioni sull'utilizzo della AWS Site-to-Site VPN con AWS Transit Gateway, consulta gli allegati AWS Site-to-Site VPN in Amazon VPC Transit Gateways nella Transit Gateway User Guide. Amazon VPC

> **Note**
>
> Amazon EVS non supporta la connettività tramite un'interfaccia virtuale privata (VIF) AWS Direct Connect o tramite una connessione AWS Site-to-Site VPN che termina direttamente nel VPC sottostante.

Configura un'istanza VPC Route Server con endpoint e peer

Amazon EVS utilizza Amazon VPC Route Server per abilitare il routing dinamico basato su BGP verso la tua rete overlay VPC. È necessario specificare un server di routing che condivida le rotte

verso almeno due endpoint del server di routing nella sottorete di accesso al servizio. L'ASN peer configurato sui peer del server di routing deve corrispondere e gli indirizzi IP peer devono essere univoci.

Se si sta configurando Route Server per la connettività Internet HCX, è necessario configurare le propagazioni del Route Server sia per la sottorete di accesso al servizio che per la sottorete pubblica che avete creato nel primo passaggio di questa procedura.

Important

L'implementazione del tuo ambiente fallisce se non soddisfi questi requisiti di Amazon EVS per la configurazione del VPC Route Server:

- È necessario configurare almeno due endpoint del server di routing nella sottorete di accesso al servizio.
- Quando si configura Border Gateway Protocol (BGP) per il gateway Tier-0, il valore ASN peer di VPC Route Server deve corrispondere al valore ASN peer di NSX Edge.
- Quando si creano i due peer del server di routing, è necessario utilizzare un indirizzo IP univoco dalla VLAN uplink NSX per ogni endpoint. Questi due indirizzi IP verranno assegnati ai bordi NSX durante l'implementazione dell'ambiente Amazon EVS.
- Quando abiliti la propagazione del Route Server, devi assicurarti che tutte le tabelle di routing che vengono propagate abbiano almeno un'associazione di sottorete esplicita. La pubblicità delle rotte BGP fallisce se le tabelle di routing propagate non hanno un'associazione di sottorete esplicita.

Per ulteriori informazioni sulla configurazione del Route Server VPC, consulta il tutorial introduttivo su Route Server.

Important

Quando abiliti la propagazione del Route Server, assicurati che tutte le tabelle di route che vengono propagate abbiano almeno un'associazione di sottorete esplicita. La pubblicità delle rotte BGP fallisce se la tabella di routing ha un'associazione di sottorete esplicita.

> **Note**
>
> Per il rilevamento della peer liveness di Route Server, Amazon EVS supporta solo il meccanismo keepalive BGP predefinito. Amazon EVS non supporta il rilevamento dell'inoltro bidirezionale (BFD) multi-hop.

> **Note**
>
> Ti consigliamo di abilitare i percorsi persistenti per l'istanza del server di routing con una durata di persistenza compresa tra 1 e 5 minuti. Se abilitata, le rotte verranno conservate nel database di routing del server di routing anche se tutte le sessioni BGP terminano. Per ulteriori informazioni, consulta Create a route server nella Guida per l' Amazon VPC utente.

> **Note**
>
> Se utilizzi un gateway NAT o un gateway di transito, assicurati che il server di routing sia configurato correttamente per propagare le route NSX alle tabelle di routing VPC.

Risoluzione dei problemi

In caso di problemi:

- Verifica che ogni tabella di routing abbia un'associazione di sottorete esplicita.
- Verifica che i valori ASN peer immessi per il server di routing e il gateway NSX Tier-0 corrispondano.
- Verificate che gli indirizzi IP degli endpoint del Route Server siano univoci.
- Controlla lo stato di propagazione delle rotte nelle tabelle delle rotte.
- Utilizza la registrazione peer di VPC Route Server per monitorare lo stato della sessione BGP e risolvere i problemi di connessione. Per ulteriori informazioni, consulta Route Server peer logging nella Amazon VPC User Guide.

Crea un ACL di rete per controllare il traffico della sottorete VLAN di Amazon EVS

Amazon EVS utilizza una lista di controllo degli accessi alla rete (ACL) per controllare il traffico da e verso le sottoreti VLAN di Amazon EVS. Puoi utilizzare l'ACL di rete predefinito per il tuo VPC oppure puoi creare un ACL di rete personalizzato per il tuo VPC con regole simili a quelle per i tuoi gruppi di sicurezza per aggiungere un livello di sicurezza al tuo VPC. Per ulteriori informazioni, consulta Creare un ACL di rete per il tuo VPC nella Amazon VPC User Guide.

Se prevedi di configurare la connettività Internet HCX, assicurati che le regole ACL di rete che configuri consentano le connessioni in entrata e in uscita necessarie per i componenti HCX. Per ulteriori informazioni sui requisiti delle porte HCX, consulta la Guida per l'utente di HCX. VMware

Important

Se ti connetti tramite Internet, l'associazione di un indirizzo IP elastico a una VLAN fornisce l'accesso diretto a Internet a tutte le risorse su quella sottorete VLAN. Assicurati di disporre di elenchi di controllo degli accessi alla rete configurati in modo da limitare l'accesso in base alle esigenze di sicurezza.

Important

I gruppi di sicurezza EC2 non funzionano su interfacce di rete elastiche collegate alle sottoreti VLAN di Amazon EVS. Per controllare il traffico da e verso le sottoreti VLAN di Amazon EVS, devi utilizzare una lista di controllo dell'accesso alla rete.

Crea un ambiente Amazon EVS

Important

Per iniziare nel modo più semplice e veloce possibile, questo argomento include i passaggi per creare un ambiente Amazon EVS con impostazioni predefinite. Prima di creare un ambiente, ti consigliamo di acquisire familiarità con tutte le impostazioni e di implementare un ambiente con le impostazioni che soddisfano i tuoi requisiti. Gli ambienti possono essere configurati solo durante la creazione iniziale dell'ambiente. Gli ambienti non possono

essere modificati dopo averli creati. Per una panoramica di tutte le possibili impostazioni dell'ambiente Amazon EVS, consulta la Amazon EVS API Reference Guide.

> **Note**
>
> L'ID dell'ambiente sarà disponibile per Amazon EVS in tutte le AWS regioni per esigenze di conformità delle licenze VCF.

> **Note**
>
> Gli ambienti Amazon EVS devono essere distribuiti nella stessa regione e zona di disponibilità delle sottoreti VPC e VPC.

Completa questo passaggio per creare un ambiente Amazon EVS con host e sottoreti VLAN.

Example

Amazon EVS console

1. Vai alla console Amazon EVS.

   > **Note**
   >
   > Assicurati che la AWS regione mostrata in alto a destra della console sia la AWS regione in cui desideri creare il tuo ambiente. In caso contrario, scegli il menu a discesa accanto al nome AWS della regione e scegli la AWS regione che desideri utilizzare.

2. Nel riquadro di navigazione, selezionare Compute environments (Ambienti di calcolo).
3. Seleziona Create environment (Crea ambiente).
4. Nella pagina Convalida dei requisiti di Amazon EVS, verifica che i requisiti di servizio siano stati soddisfatti. Per ulteriori informazioni, consulta Configurazione di Amazon Elastic VMware Service.
   a. (Facoltativo) In Nome, inserisci un nome di ambiente.
   b. Per la versione Environment, scegli la tua versione VCF. Per informazioni sulle versioni VCF fornite da Amazon EVS, consulta. the section called "Versioni VCF e istanze EC2"

c. Per Site ID, inserisci il tuo ID del sito Broadcom.

d. Per la chiave della soluzione VCF, immettere una chiave di soluzione VCF (VMware vSphere 8 Enterprise Plus for VCF). Questa chiave di licenza non può essere utilizzata da un ambiente esistente.

> **Note**
>
> La chiave della soluzione VCF deve avere core sufficienti. Per ulteriori informazioni, consulta the section called "Abbonamenti VCF".

> **Note**
>
> La tua licenza VCF sarà disponibile per Amazon EVS in tutte le AWS regioni per garantire la conformità delle licenze. Amazon EVS non convalida le chiavi di licenza. Per convalidare le chiavi di licenza, visita l'assistenza Broadcom.

> **Note**
>
> Amazon EVS richiede il mantenimento di una chiave di soluzione VCF valida in SDDC Manager per il corretto funzionamento del servizio. Se si gestisce la chiave della soluzione VCF utilizzando vSphere Client dopo la distribuzione, è necessario assicurarsi che le chiavi vengano visualizzate anche nella schermata delle licenze dell'interfaccia utente di SDDC Manager.

e. Per la chiave di licenza vSAN, inserire una chiave di licenza vSAN. Questa chiave di licenza non può essere utilizzata da un ambiente esistente.

> **Note**
>
> La chiave di licenza vSAN deve avere una capacità vSAN sufficiente. Per ulteriori informazioni, consulta the section called "Abbonamenti VCF".

> **Note**
>
> La tua licenza VCF sarà disponibile per Amazon EVS in tutte le AWS regioni per garantire la conformità delle licenze. Amazon EVS non convalida le chiavi di licenza. Per convalidare le chiavi di licenza, visita l'assistenza Broadcom.

> **Note**
>
> Amazon EVS richiede il mantenimento di una chiave di licenza vSAN valida in SDDC Manager per scegliere il servizio per il corretto funzionamento. Se si gestisce la chiave di licenza vSAN utilizzando vSphere Client dopo la distribuzione, è necessario assicurarsi che le chiavi vengano visualizzate anche nella schermata delle licenze dell'interfaccia utente di SDDC Manager.

f. Per quanto riguarda i termini della licenza VCF, seleziona la casella per confermare che hai acquistato e continuerai a mantenere il numero richiesto di licenze software VCF per coprire tutti i core dei processori fisici nell'ambiente Amazon EVS. Le informazioni sul tuo software VCF in Amazon EVS verranno condivise con Broadcom per verificare la conformità della licenza.

g. Scegli Next (Successivo).

5. Nella pagina Specificare i dettagli dell'host, completa i seguenti passaggi quattro volte per aggiungere quattro host all'ambiente. Gli ambienti Amazon EVS richiedono quattro host per la distribuzione iniziale.

   a. Scegli Aggiungi dettagli sull'host.

   b. Per il nome host DNS, inserisci il nome host dell'host.

   c. Per il tipo di istanza, scegli il tipo di istanza EC2.

   d. Per la versione host ESX, durante la creazione dell'ambiente verrà utilizzata una versione ESX predefinita per la versione VCF scelta. Per ulteriori informazioni, consulta the section called “Versioni VCF e istanze EC2”.

> **Important**
>
> Non interrompere o terminare le istanze EC2 distribuite da Amazon EVS. Questa azione comporta la perdita di dati.

e. Per la coppia di chiavi SSH, scegli una coppia di chiavi SSH per l'accesso SSH all'host.

f. Scegli Aggiungi host.

6. Nella pagina Configura reti e connettività, procedi come segue.

a. Per i requisiti di connettività HCX, seleziona se desideri utilizzare HCX con connettività privata o tramite Internet.

b. Per VPC, scegli il VPC che hai creato in precedenza.

c. (Solo per la connettività Internet HCX) Per l'ACL di rete HCX, scegli a quale ACL di rete sarà associata la tua VLAN HCX.

> **Important**
>
> Ti consigliamo vivamente di creare un ACL di rete personalizzato dedicato alla VLAN HCX. Per ulteriori informazioni, consulta the section called "Configura l'ACL di rete".

d. Per la sottorete di accesso al servizio, scegli la sottorete privata creata al momento della creazione del VPC.

e. Per il gruppo di sicurezza: facoltativo, puoi scegliere fino a due gruppi di sicurezza che controllano la comunicazione tra il piano di controllo di Amazon EVS e il VPC. Amazon EVS utilizza il gruppo di sicurezza predefinito se non viene scelto alcun gruppo di sicurezza.

> **Note**
>
> Assicurati che i gruppi di sicurezza scelti forniscano connettività ai tuoi server DNS e alle sottoreti VLAN Amazon EVS.

f. In Connettività di gestione, inserisci i blocchi CIDR da utilizzare per le sottoreti VLAN di Amazon EVS. Per il blocco CIDR VLAN HCX uplink, se si configura una VLAN HCX pubblica, è necessario specificare un blocco CIDR con una lunghezza della maschera di rete esattamente /28. Amazon EVS genera un errore di convalida se viene specificata un'altra dimensione di blocco CIDR per la VLAN HCX pubblica. Per una VLAN HCX privata e tutti gli

altri blocchi VLANs CIDR, la lunghezza minima della maschera di rete che puoi usare è /28 e la massima è /24.

> **Important**
>
> Le sottoreti VLAN Amazon EVS possono essere create solo durante la creazione dell'ambiente Amazon EVS e non possono essere modificate dopo la creazione dell'ambiente. È necessario assicurarsi che i blocchi CIDR della sottorete VLAN siano dimensionati correttamente prima di creare l'ambiente. Non sarà possibile aggiungere sottoreti VLAN dopo la distribuzione dell'ambiente. Per ulteriori informazioni, consulta the section called "Considerazioni sulla rete Amazon EVS".

g. In Espansione VLANs, inserisci i blocchi CIDR per ulteriori sottoreti VLAN Amazon EVS che possono essere utilizzate per espandere le funzionalità VCF all'interno di Amazon EVS, ad esempio abilitando NSX Federation.

h. In Connettività Workload/VCF, inserisci il blocco CIDR per la VLAN di uplink NSX e scegli due endpoint VPC Route Server peer that peer to Route Server IDs tramite l'uplink NSX.

> **Note**
>
> Amazon EVS richiede un'istanza VPC Route Server associata a due endpoint Route Server e due peer Route Server prima della distribuzione EVS. Questa configurazione consente il routing dinamico basato su BGP sull'uplink NSX. Per ulteriori informazioni, consulta the section called "Configura un'istanza VPC Route Server con endpoint e peer".

i. Scegli Next (Successivo).

7. Nella pagina Specificare i nomi host DNS di gestione, procedi come segue.

a. In Nomi host DNS delle appliance di gestione, inserisci i nomi host DNS delle macchine virtuali su cui ospitare i dispositivi di gestione VCF. Se utilizzi Route 53 come provider DNS, scegli anche la zona ospitata che contiene i tuoi record DNS.

b. In Credenziali, scegli se utilizzare la chiave KMS AWS gestita per Secrets Manager o una chiave KMS gestita dal cliente fornita da te. Questa chiave viene utilizzata per crittografare le credenziali VCF necessarie per utilizzare le appliance SDDC Manager, NSX Manager e vCenter.

> **Note**
>
> Esistono costi di utilizzo associati alle chiavi KMS gestite dal cliente. Per ulteriori informazioni, consulta la pagina dei prezzi di AWS KMS.

c. Scegli Next (Successivo).

8. (Facoltativo) Nella pagina Aggiungi tag, aggiungi i tag che desideri assegnare a questo ambiente e scegli Avanti.

> **Note**
>
> Gli host creati come parte di questo ambiente riceveranno il seguente tag:`DoNotDelete-EVS-<environmentid>-<hostname>`.

> **Note**
>
> I tag associati all'ambiente Amazon EVS non si propagano alle AWS risorse sottostanti come le istanze EC2. Puoi creare tag sulle AWS risorse sottostanti utilizzando la rispettiva console di servizio o il. AWS CLI

9. Nella pagina Rivedi e crea, rivedi la configurazione e scegli Crea ambiente.

> **Important**
>
> Durante la distribuzione dell'ambiente, Amazon EVS crea le sottoreti VLAN EVS e le associa implicitamente alla tabella di routing principale. Una volta completata la distribuzione, devi associare esplicitamente le sottoreti VLAN di Amazon EVS a una tabella di routing per scopi di connettività NSX. Per ulteriori informazioni, consulta the section called "Associa esplicitamente le sottoreti VLAN di Amazon EVS a una tabella di routing VPC".

> **Note**
>
> Amazon EVS distribuisce una recente versione in bundle di VMware Cloud Foundation che potrebbe non includere aggiornamenti di singoli prodotti, noti come patch

asincrone. Al termine di questa distribuzione, consigliamo vivamente di esaminare e aggiornare i singoli prodotti utilizzando l'Async Patch Tool (AP Tool) di Broadcom o l'automazione LCM integrata nel prodotto SDDC Manager. Gli aggiornamenti di NSX devono essere eseguiti all'esterno di SDDC Manager.

> **Note**
>
> La creazione dell'ambiente può richiedere diverse ore.

AWS CLI

1. Aprire una sessione di terminale.
2. Crea un ambiente Amazon EVS. Di seguito è riportato un esempio di `aws evs create-environment` richiesta.

> **Important**
>
> Prima di eseguire il `aws evs create-environment` comando, verifica che tutti i prerequisiti di Amazon EVS siano soddisfatti. La distribuzione dell'ambiente fallisce se i prerequisiti non sono stati soddisfatti. Per ulteriori informazioni, consulta Configurazione di Amazon Elastic VMware Service.

> **Important**
>
> Durante la distribuzione dell'ambiente, Amazon EVS crea le sottoreti VLAN EVS e le associa implicitamente alla tabella di routing principale. Una volta completata la distribuzione, devi associare esplicitamente le sottoreti VLAN di Amazon EVS a una tabella di routing per scopi di connettività NSX. Per ulteriori informazioni, consulta the section called "Associa esplicitamente le sottoreti VLAN di Amazon EVS a una tabella di routing VPC".

> **Note**
>
> Amazon EVS distribuisce una recente versione in bundle di VMware Cloud Foundation che potrebbe non includere aggiornamenti di singoli prodotti, noti come patch asincrone. Al termine di questa distribuzione, ti consigliamo vivamente di rivedere e aggiornare i singoli prodotti utilizzando l'Async Patch Tool (AP Tool) di Broadcom o l'automazione LCM integrata nel prodotto SDDC Manager. Gli aggiornamenti di NSX devono essere eseguiti all'esterno di SDDC Manager.

> **Note**
>
> L'implementazione dell'ambiente può richiedere diverse ore.

- Per`--vpc-id`, specifica il VPC che hai creato in precedenza con un intervallo IPv4 CIDR minimo di /22.
- Per`--service-access-subnet-id`, specifica l'ID univoco della sottorete privata creata quando hai creato il VPC.
- Per`--vcf-version`, vedi the section called “Versioni VCF e istanze EC2” per le versioni VCF fornite da Amazon EVS,
- Con`--terms-accepted`, confermi di aver acquistato e continuerai a mantenere il numero richiesto di licenze software VCF per coprire tutti i core dei processori fisici nell'ambiente Amazon EVS. Le informazioni sul tuo software VCF in Amazon EVS verranno condivise con Broadcom per verificare la conformità della licenza.
- Per`--license-info`, inserisci la chiave della soluzione VCF (VMware vSphere 8 Enterprise Plus for VCF) e la chiave di licenza vSAN.

  > **Note**
  >
  > I requisiti per la chiave della soluzione VCF (incluso il numero minimo di core) e la chiave di licenza vSAN (inclusa la capacità minima di vSAN) variano a seconda del tipo di istanza. Per le soglie specifiche per la configurazione, consulta. the section called “Abbonamenti VCF”

> **Note**
>
> Amazon EVS richiede di mantenere una chiave di soluzione VCF e una chiave di licenza vSAN valide in SDDC Manager per il corretto funzionamento del servizio. Se si gestiscono queste chiavi di licenza utilizzando vSphere Client dopo la distribuzione, è necessario assicurarsi che vengano visualizzate anche nella schermata delle licenze dell'interfaccia utente di SDDC Manager.

> **Note**
>
> La chiave della soluzione VCF e la chiave di licenza vSAN non possono essere utilizzate da un ambiente Amazon EVS esistente.

- Per `--initial-vlans` specificare gli intervalli CIDR per le sottoreti VLAN Amazon EVS che Amazon EVS crea per tuo conto. VLANs Vengono utilizzati per distribuire dispositivi di gestione VCF. Se si configura una VLAN HCX pubblica, è necessario specificare un blocco CIDR con una lunghezza della maschera di rete esattamente /28. Amazon EVS genera un errore di convalida se viene specificata un'altra dimensione di blocco CIDR per la VLAN HCX pubblica. Per una VLAN HCX privata e tutti gli altri blocchi VLANs CIDR, la lunghezza minima della maschera di rete che puoi usare è /28 e la massima è /24.
- `hcxNetworkAclId`viene utilizzato per configurare la connettività Internet HCX. Specificare un ACL di rete personalizzato per la VLAN HCX pubblica.

> **Important**
>
> Si consiglia vivamente di creare un ACL di rete personalizzato dedicato alla VLAN HCX. Per ulteriori informazioni, consulta the section called “Configura l'ACL di rete”.

> **Important**
>
> Le sottoreti VLAN Amazon EVS possono essere create solo durante la creazione dell'ambiente Amazon EVS e non possono essere modificate dopo la creazione dell'ambiente. È necessario assicurarsi che i blocchi CIDR della sottorete VLAN

siano dimensionati correttamente prima di creare l'ambiente. Non sarà possibile aggiungere sottoreti VLAN dopo la distribuzione dell'ambiente. Per ulteriori informazioni, consulta the section called "Considerazioni sulla rete Amazon EVS".

- Per `--hosts`, specifica i dettagli degli host richiesti da Amazon EVS per la distribuzione dell'ambiente. Includi il nome host DNS, il nome della chiave SSH EC2 e il tipo di istanza EC2 per ogni host. L'ID host dedicato è facoltativo.

  Important

  Non interrompere o terminare le istanze EC2 distribuite da Amazon EVS. Questa azione comporta la perdita di dati.

- Per `--connectivity-info`, specifica il peer 2 VPC Route Server IDs che hai creato nel passaggio precedente.

  Note

  Amazon EVS richiede un'istanza VPC Route Server associata a due endpoint Route Server e due peer Route Server prima della distribuzione EVS. Questa configurazione consente il routing dinamico basato su BGP sull'uplink NSX. Per ulteriori informazioni, consulta the section called "Configura un'istanza VPC Route Server con endpoint e peer".

- Per `--vcf-hostnames`, inserisci i nomi host DNS per le macchine virtuali su cui ospitare i dispositivi di gestione VCF.
- Per `--site-id`, inserisci l'ID univoco del tuo sito Broadcom. Questo ID consente l'accesso al portale Broadcom e viene fornito da Broadcom al momento della stipula del contratto software o del rinnovo del contratto.
- (Facoltativo) Per `--region`, inserisci la regione in cui verrà distribuito l'ambiente. Se la regione non è specificata, viene utilizzata la regione predefinita.

```
aws evs create-environment \
--environment-name testEnv \
--vpc-id vpc-1234567890abcdef0 \
--service-access-subnet-id subnet-01234a1b2cde1234f \
--vcf-version VCF-5.2.2 \
--terms-accepted \
```

```
--license-info "{
      \"solutionKey\": \"00000-00000-00000-abcde-11111\",
      \"vsanKey\": \"00000-00000-00000-abcde-22222\"
    }" \
   --initial-vlans "{
      \"isHcxPublic\": true,
      \"hcxNetworkAclId\": \"nacl-abcd1234\",
      \"vmkManagement\": {
        \"cidr\": \"10.10.0.0/24\"
      },
      \"vmManagement\": {
        \"cidr\": \"10.10.1.0/24\"
      },
      \"vMotion\": {
        \"cidr\": \"10.10.2.0/24\"
      },
      \"vSan\": {
        \"cidr\": \"10.10.3.0/24\"
      },
      \"vTep\": {
        \"cidr\": \"10.10.4.0/24\"
      },
      \"edgeVTep\": {
        \"cidr\": \"10.10.5.0/24\"
      },
      \"nsxUplink\": {
        \"cidr\": \"10.10.6.0/24\"
      },
      \"hcx\": {
        \"cidr\": \"10.10.7.0/24\"
      },
      \"expansionVlan1\": {
        \"cidr\": \"10.10.8.0/24\"
      },
      \"expansionVlan2\": {
          \"cidr\": \"10.10.9.0/24\"
      }
    }" \
--hosts "[
    {
      \"hostName\": \"esx01\",
      \"keyName\": \"sshKey-04-05-45\”,
      \"instanceType\": \"i4i.metal\",
      \"dedicatedHostId\": \"h-07879acf49EXAMPLE\"
```

```
    },
    {
      \"hostName\": \"esx02\",
      \"keyName\": \"sshKey-04-05-45\",
      \"instanceType\": \"i4i.metal\",
      \"dedicatedHostId\": \"h-07878bde50EXAMPLE\"
    },
    {
      \"hostName\": \"esx03\",
      \"keyName\": \"sshKey-04-05-45\",
      \"instanceType\": \"i4i.metal\",
      \"dedicatedHostId\": \"h-07877eio51EXAMPLE\"
    },
    {
      \"hostName\": \"esx04\",
      \"keyName\": \"sshKey-04-05-45\",
      \"instanceType\": \"i4i.metal\",
      \"dedicatedHostId\": \"h-07863ghi52EXAMPLE\"
    }
  ]" \
--connectivity-info "{
    \"privateRouteServerPeerings\": [\"rsp-1234567890abcdef0\",\"rsp-
abcdef01234567890\"]
  }" \
  --vcf-hostnames "{
    \"vCenter\": \"vcf-vc01\",
    \"nsx\": \"vcf-nsx\",
    \"nsxManager1\": \"vcf-nsxm01\",
    \"nsxManager2\": \"vcf-nsxm02\",
    \"nsxManager3\": \"vcf-nsxm03\",
    \"nsxEdge1\": \"vcf-edge01\",
    \"nsxEdge2\": \"vcf-edge02\",
    \"sddcManager\": \"vcf-sddcm01\",
    \"cloudBuilder\": \"vcf-cb01\"
  }" \
--site-id my-site-id \
--region us-east-2
```

Di seguito è riportata una risposta di esempio.

```
{
    "environment": {
        "environmentId": "env-abcde12345",
```

```
        "environmentState": "CREATING",
        "stateDetails": "The environment is being initialized, this operation
 may take some time to complete.",
        "createdAt": "2025-04-13T12:03:39.718000+00:00",
        "modifiedAt": "2025-04-13T12:03:39.718000+00:00",
        "environmentArn": "arn:aws:evs:us-east-2:111122223333:environment/env-
abcde12345",
        "environmentName": "testEnv",
        "vpcId": "vpc-1234567890abcdef0",
        "serviceAccessSubnetId": "subnet-01234a1b2cde1234f",
        "vcfVersion": "VCF-5.2.2",
        "termsAccepted": true,
        "licenseInfo": [
            {
                "solutionKey": "00000-00000-00000-abcde-11111",
                "vsanKey": "00000-00000-00000-abcde-22222"
            }
        ],
        "siteId": "my-site-id",
        "connectivityInfo": {
            "privateRouteServerPeerings": [
                "rsp-1234567890abcdef0",
                "rsp-abcdef01234567890"
            ]
        },
        "vcfHostnames": {
            "vCenter": "vcf-vc01",
            "nsx": "vcf-nsx",
            "nsxManager1": "vcf-nsxm01",
            "nsxManager2": "vcf-nsxm02",
            "nsxManager3": "vcf-nsxm03",
            "nsxEdge1": "vcf-edge01",
            "nsxEdge2": "vcf-edge02",
            "sddcManager": "vcf-sddcm01",
            "cloudBuilder": "vcf-cb01"
        }
    }
}
```

Verifica la creazione dell'ambiente Amazon EVS

Example

Amazon EVS console

1. Vai alla console Amazon EVS.
2. Nel riquadro di navigazione, selezionare Compute environments (Ambienti di calcolo).
3. Seleziona l'ambiente.
4. Seleziona la scheda Dettagli.
5. Verifica che lo stato dell'ambiente sia passato e che lo stato dell'ambiente sia stato creato. Ciò consente di sapere che l'ambiente è pronto per l'uso.

> **Note**
>
> La creazione dell'ambiente può richiedere diverse ore. Se lo stato Ambiente mostra ancora Creazione, aggiorna la pagina.

AWS CLI

1. Aprire una sessione terminale.
2. Esegui il comando seguente, utilizzando l'ID dell'ambiente e il nome della regione che contiene le tue risorse. L'ambiente è pronto per l'uso quando lo `environmentState` è`CREATED`.

> **Note**
>
> La creazione dell'ambiente può richiedere diverse ore. Se viene visualizzato un immagine `environmentState` `CREATING` fissa, esegui nuovamente il comando per aggiornare l'output.

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

Di seguito è riportata una risposta di esempio.

```
{
```

```
    "environment": {
        "environmentId": "env-abcde12345",
        "environmentState": "CREATED",
        "createdAt": "2025-04-13T13:39:49.546000+00:00",
        "modifiedAt": "2025-04-13T13:40:39.355000+00:00",
        "environmentArn": "arn:aws:evs:us-east-2:111122223333:environment/env-
abcde12345",
        "environmentName": "testEnv",
        "vpcId": "vpc-0c6def5b7b61c9f41",
        "serviceAccessSubnetId": "subnet-06a3c3b74d36b7d5e",
        "vcfVersion": "VCF-5.2.2",
        "termsAccepted": true,
        "licenseInfo": [
            {
                "solutionKey": "00000-00000-00000-abcde-11111",
                "vsanKey": "00000-00000-00000-abcde-22222"
            }
        ],
        "siteId": "my-site-id",
        "checks": [],
        "connectivityInfo": {
            "privateRouteServerPeerings": [
                "rsp-056b2b1727a51e956",
                "rsp-07f636c5150f171c3"
            ]
        },
        "vcfHostnames": {
            "vCenter": "vcf-vc01",
            "nsx": "vcf-nsx",
            "nsxManager1": "vcf-nsxm01",
            "nsxManager2": "vcf-nsxm02",
            "nsxManager3": "vcf-nsxm03",
            "nsxEdge1": "vcf-edge01",
            "nsxEdge2": "vcf-edge02",
            "sddcManager": "vcf-sddcm01",
            "cloudBuilder": "vcf-cb01"
        },
        "credentials": []
    }
}
```

Associa esplicitamente le sottoreti VLAN di Amazon EVS a una tabella di routing VPC

Associa esplicitamente ciascuna delle sottoreti VLAN di Amazon EVS a una tabella di routing nel tuo VPC. Questa tabella di routing viene utilizzata per consentire alle AWS risorse di comunicare con macchine virtuali su segmenti di rete NSX, in esecuzione con Amazon EVS. Se hai creato una VLAN HCX pubblica, assicurati di associare esplicitamente la sottorete VLAN HCX pubblica a una tabella di routing pubblica nel tuo VPC che indirizza verso un gateway Internet.

Example

Amazon VPC console

1. Vai alla console VPC.
2. Nel riquadro di navigazione, seleziona Tabelle di routing.
3. Scegli la tabella di routing che desideri associare alle sottoreti VLAN di Amazon EVS.
4. Seleziona la scheda Associazioni delle sottoreti.
5. In Associazioni di sottoreti esplicite, seleziona Modifica associazioni di sottoreti.
6. Seleziona tutte le sottoreti VLAN di Amazon EVS.
7. Scegli Salva associazioni.

AWS CLI

1. Apri una sessione terminale.
2. Identifica la sottorete VLAN di Amazon EVS. IDs

```
aws ec2 describe-subnets
```

3. Associa le sottoreti VLAN di Amazon EVS a una tabella di routing nel tuo VPC.

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

EIPs Associa alla sottorete VLAN pubblica HCX (per la connettività Internet HCX)

Segui questi passaggi per associare l'indirizzo IP elastico (EIPs) dal pool IPAM alla VLAN pubblica HCX per la connettività Internet HCX. È necessario associarne almeno due EIPs per i dispositivi HCX Manager e HCX Interconnect (HCX-IX). Associa un EIP aggiuntivo per ogni appliance di rete HCX che devi implementare. È possibile avere fino a 13 EIPs dal pool IPAM associati alla VLAN pubblica HCX.

Important

La connettività Internet pubblica HCX fallisce se non si associano almeno due del pool IPAM a una EIPs sottorete VLAN pubblica HCX.

Note

Al momento Amazon EVS supporta solo l'associazione EIPs alla VLAN HCX.

Note

Non è possibile associare i primi due EIPs o gli ultimi EIP del blocco CIDR IPAM pubblico alla sottorete VLAN. Questi EIPs sono riservati come indirizzi di rete, gateway predefiniti e indirizzi di trasmissione. Amazon EVS genera un errore di convalida se tenti di EIPs associarli alla sottorete VLAN.

Amazon EVS console

1. Vai alla console Amazon EVS.
2. Nel menu di navigazione, scegli Ambienti.
3. Seleziona l'ambiente.
4. Nella scheda Reti e connettività, seleziona la VLAN pubblica HCX.
5. Scegli Associa EIP a VLAN.
6. Seleziona gli indirizzi IP elastici da associare alla VLAN pubblica HCX.
7. Selezionare Associate (Associa) EIPs.

8. Controlla le associazioni EIP per confermare che siano EIPs state associate alla VLAN pubblica HCX.

AWS CLI

1. Per associare un indirizzo IP elastico a una VLAN, usa il comando example. `associate-eip-to-vlan`
   - `environment-id`- L'ID del tuo ambiente Amazon EVS.
   - `vlan-name`- Il nome della VLAN da associare all'indirizzo IP elastico.
   - `allocation-id`- L'ID di allocazione dell'indirizzo IP elastico.

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

   Il comando restituisce dettagli sulla VLAN, inclusa la nuova associazione EIP:

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

L'`eipAssociations`array mostra la nuova associazione, tra cui:

- `associationId`- L'ID univoco di questa associazione EIP, utilizzato per la dissociazione.
- `allocationId`- L'ID di allocazione dell'indirizzo IP elastico associato.
- `ipAddress`- L'indirizzo IP assegnato alla VLAN.

2. Ripetere il passaggio per associarne altri EIPs.

Configurazione delle tabelle di routing del gateway di transito e dei prefissi Direct Connect per la connettività locale (opzionale)

Se stai configurando la connettività di rete locale utilizzando Direct Connect o una AWS Site-to-Site VPN con un gateway di transito, devi aggiornare le tabelle di routing del gateway di transito con il VPC creato CIDRs nell'ambiente Amazon EVS. Per ulteriori informazioni, consulta le tabelle di routing dei gateway di transito di Amazon VPC in Amazon VPC.

Se utilizzi AWS Direct Connect, potrebbe essere necessario aggiornare anche i prefissi Direct Connect per inviare e ricevere percorsi aggiornati dal VPC. Per ulteriori informazioni, consulta Consenti interazioni con prefissi per i gateway AWS Direct Connect.

Recupera le credenziali VCF e accedi ai dispositivi di gestione VCF

Amazon EVS utilizza AWS Secrets Manager per creare, crittografare e archiviare segreti gestiti nel tuo account. Questi segreti contengono le credenziali VCF necessarie per installare e accedere ai dispositivi di gestione VCF come vCenter Server, NSX e SDDC Manager, nonché la password root ESX. Per ulteriori informazioni sul recupero dei segreti, consulta Ottieni AWS segreti da Secrets Manager nella Guida per l'utente di AWS Secrets Manager.

> **Note**
>
> Amazon EVS non fornisce una rotazione gestita dei segreti. Si consiglia di ruotare regolarmente i segreti su una finestra di rotazione prestabilita per assicurarsi che i segreti non durino a lungo.

Dopo aver recuperato le credenziali VCF da AWS Secrets Manager, è possibile utilizzarle per accedere ai dispositivi di gestione VCF. Per ulteriori informazioni, vedere Accesso all'interfaccia

utente di SDDC Manager e Come utilizzare e configurare il client vSphere nella documentazione VMware del prodotto.

Configura la console seriale EC2 (opzionale)

Per impostazione predefinita, Amazon EVS abilita ESX Shell sugli host Amazon EVS appena distribuiti. Questa configurazione consente l'accesso alla porta seriale dell'istanza Amazon EC2 tramite la console seriale EC2, che puoi utilizzare per risolvere problemi di avvio, configurazione di rete e altri problemi. La console seriale non richiede che l'istanza abbia funzionalità di rete. Con la console seriale, puoi inserire comandi a un'istanza EC2 in esecuzione come se la tastiera e il monitor fossero collegati direttamente alla porta seriale dell'istanza.

È possibile accedere alla console seriale EC2 utilizzando la console EC2 o il. AWS CLI Per ulteriori informazioni, consulta la Console seriale EC2 per le istanze nella Guida per l'utente di Amazon EC2.

> **Note**
>
> La console seriale EC2 è l'unico meccanismo supportato da Amazon EVS per accedere alla Direct Console User Interface (DCUI) per interagire con un host ESX a livello locale.

> **Note**
>
> Amazon EVS disabilita SSH remoto per impostazione predefinita. Per ulteriori informazioni sull'abilitazione di SSH per accedere alla shell ESX remota, vedere Accesso remoto alla shell ESX con SSH nella documentazione del prodotto VMware vSphere.

Connect alla console seriale EC2

Per connettersi alla console seriale EC2 e utilizzare lo strumento scelto per la risoluzione dei problemi, è necessario completare alcune attività preliminari. Per ulteriori informazioni, consulta Prerequisiti per la console seriale EC2 e Connect to the EC2 Serial Console nella Amazon EC2 User Guide.

> **Note**
>
> Per connettersi alla console seriale EC2, lo stato dell'istanza EC2 deve essere. `running` Non puoi connetterti alla console seriale se l'istanza si trova nello stato`pending`,`stopping`,

`stoppedshutting-down`, `oterminated`. Per ulteriori informazioni sulle modifiche dello stato dell'istanza, consulta la modifica dello stato dell'istanza di Amazon EC2 nella Amazon EC2 User Guide.

Configura l'accesso alla console seriale EC2

Per configurare l'accesso alla console seriale EC2, tu o il tuo amministratore dovete concedere l'accesso alla console seriale a livello di account e quindi configurare le policy IAM per concedere l'accesso ai vostri utenti. Per le istanze Linux, devi anche configurare un utente basato su password su ogni istanza in modo che gli utenti possano utilizzare la console seriale per la risoluzione dei problemi. Per ulteriori informazioni, consulta Configurare l'accesso alla console seriale EC2 nella Guida per l'utente di Amazon EC2.

Eliminazione

Segui questi passaggi per eliminare le AWS risorse che sono state create.

Eliminare gli host e l'ambiente Amazon EVS

Segui questi passaggi per eliminare gli host e l'ambiente Amazon EVS. Questa azione elimina l'installazione VMware VCF in esecuzione nel tuo ambiente Amazon EVS.

> **Note**
>
> Per eliminare un ambiente Amazon EVS, devi prima eliminare tutti gli host all'interno dell'ambiente. Un ambiente non può essere eliminato se vi sono host associati all'ambiente.

Example

Amazon EVS console

1. Vai alla console Amazon EVS.
2. Nel pannello di navigazione, scegli Ambiente.
3. Seleziona l'ambiente che contiene gli host da eliminare.
4. Seleziona la scheda Host.

5. Seleziona l'host e scegli Elimina nella scheda Host. Ripeti questo passaggio per ogni host dell'ambiente.
6. Nella parte superiore della pagina Ambienti, scegli Elimina e quindi Elimina ambiente.

> **Note**
>
> L'eliminazione dell'ambiente elimina anche le sottoreti VLAN di Amazon EVS e i segreti di Secrets AWS Manager creati da Amazon EVS. AWS le risorse che crei non vengono eliminate. Queste risorse possono continuare a comportare costi.

7. Se disponi di prenotazioni di capacità Amazon EC2 che non ti servono più, assicurati di averle annullate. Per ulteriori informazioni, consulta Annullamento di una prenotazione della capacità nella Guida per l'utente di Amazon EC2.

AWS CLI

1. Apri una sessione terminale.
2. Identifica l'ambiente che contiene l'host da eliminare.

```
aws evs list-environments
```

Di seguito è riportata una risposta di esempio.

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

```
            "environmentState": "CREATED",
            "createdAt": "2025-04-13T13:39:49.546000+00:00",
            "modifiedAt": "2025-04-13T13:52:13.342000+00:00",
            "environmentArn": "arn:aws:evs:us-east-2:111122223333:environment/env-
edcba54321"
        }
    ]
}
```

3. Eliminare gli host dall'ambiente. Di seguito è riportato un esempio di `aws evs delete-environment-host` richiesta.

> **Note**
>
> Per poter eliminare un ambiente, è necessario innanzitutto eliminare tutti gli host contenuti nell'ambiente.

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

4. Ripeti i passaggi precedenti per eliminare gli host rimanenti nel tuo ambiente.
5. Eliminare l'ambiente.

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

> **Note**
>
> L'eliminazione dell'ambiente elimina anche le sottoreti VLAN di Amazon EVS e i segreti di Secrets AWS Manager creati da Amazon EVS. AWS Le altre risorse che crei non vengono eliminate. Queste risorse potrebbero continuare a comportare costi.

6. Se disponi di prenotazioni di capacità Amazon EC2 che non ti servono più, assicurati di averle annullate. Per ulteriori informazioni, consulta Annullamento di una prenotazione della capacità nella Guida per l'utente di Amazon EC2.

Elimina le risorse IPAM (per la connettività Internet HCX)

Se hai configurato la connettività Internet HCX, segui questi passaggi per eliminare le risorse IPAM.

1. Rilascia le allocazioni EIP dal pool IPAM pubblico. Per ulteriori informazioni, consulta Rilasciare un'allocazione nella Guida per l'utente di VPC IP Address Manager.
2. Estraete il IPv4 CIDR pubblico dal pool IPAM. Per ulteriori informazioni, consulta Deprovisioning CIDRs da un pool nella Guida per l'utente di VPC IP Address Manager.
3. Eliminare il pool IPAM pubblico. Per ulteriori informazioni, consulta Eliminare un pool nella Guida per l'utente di VPC IP Address Manager.
4. Elimina l'IPAM. Per ulteriori informazioni, consulta Eliminare un IPAM nella Guida per l'utente di VPC IP Address Manager.

Eliminare i componenti del VPC Route Server

Per i passaggi per eliminare i componenti di Amazon VPC Route Server che hai creato, consulta la sezione Route Server cleanup nella Amazon VPC User Guide.

Elimina la lista di controllo degli accessi alla rete (ACL)

Per i passaggi per eliminare una lista di controllo degli accessi alla rete, consulta Eliminare un ACL di rete per il tuo VPC nella Amazon VPC User Guide.

Dissocia ed elimina le tabelle di routing delle sottoreti

Per i passaggi per dissociare ed eliminare le tabelle di routing di sottorete, consulta Tabelle di routing di subnet nella Amazon VPC User Guide.

Elimina le sottoreti

Elimina le sottoreti VPC, inclusa la sottorete di accesso al servizio. Per i passaggi per eliminare le sottoreti VPC, consulta Eliminare una sottorete nella Amazon VPC User Guide.

> **Note**
>
> Se utilizzi Route 53 for DNS, rimuovi gli endpoint in entrata prima di tentare di eliminare la sottorete di accesso al servizio. In caso contrario, non sarà possibile eliminare la sottorete di accesso al servizio.

> **Note**
>
> Amazon EVS elimina le sottoreti VLAN per tuo conto quando l'ambiente viene eliminato. Le sottoreti VLAN di Amazon EVS possono essere eliminate solo quando l'ambiente viene eliminato.

Eliminare il VPC

Per i passaggi per eliminare il VPC, consulta Elimina il tuo VPC nella Amazon VPC User Guide.

Fasi successive

Migra i tuoi carichi di lavoro su Amazon EVS utilizzando VMware Hybrid Cloud Extension (VMware HCX). Per ulteriori informazioni, consulta Migrazione.

Migra i carichi di lavoro su Amazon EVS utilizzando HCX VMware

Dopo l'implementazione di Amazon EVS, puoi implementare VMware HCX con connettività Internet privata o pubblica per facilitare la migrazione dei carichi di lavoro su Amazon EVS. Per ulteriori informazioni, consulta Getting Started with VMware HCX nella HCX User Guide. VMware

> **Important**
>
> La migrazione HCX basata su Internet in genere non è consigliata per:
>
> - Applicazioni sensibili al jitter o alla latenza della rete.
> - Operazioni vMotion critiche in termini di tempo.
> - Migrazioni su larga scala con requisiti prestazionali rigorosi.
>
> Per questi scenari, consigliamo di utilizzare la connettività privata HCX. Una connessione privata dedicata offre prestazioni più affidabili rispetto alle connessioni basate su Internet.

Opzioni di connettività HCX

Puoi migrare i carichi di lavoro su Amazon EVS utilizzando la connettività privata con Direct AWS Connect o connessione Site-to-Site VPN o utilizzando la connettività pubblica.

A seconda della situazione e delle opzioni di connettività, potresti preferire utilizzare la connettività pubblica o privata con HCX. Ad esempio, alcuni siti possono avere una connettività privata con una maggiore coerenza delle prestazioni, ma un throughput inferiore a causa della crittografia VPN o delle velocità di collegamento limitate. Allo stesso modo, potresti avere una connettività Internet pubblica ad alta velocità che presenta una maggiore variabilità in termini di prestazioni. Con Amazon EVS, puoi scegliere l'opzione di connettività più adatta a te.

La tabella seguente confronta le differenze tra la connettività privata e pubblica di HCX.

Connettività privata	Connettività pubblica
Panoramica	Panoramica

Connettività privata	Connettività pubblica
Utilizza solo connessioni private all'interno del VPC. Facoltativamente, puoi utilizzare AWS Direct Connect o Site-to-Site VPN con un gateway di transito per la connettività di rete esterna.	Utilizza la connettività Internet pubblica con indirizzi IP elastici, abilitando le migrazioni senza una connessione privata dedicata.
Ideale per	Ideale per
• Operazioni VMotion sensibili al fattore tempo. • Migrazioni su larga scala. • Applicazioni sensibili alla latenza/jitter. • Trasferimenti di dati ad alto volume. • Organizzazioni con AWS Direct Connect/AWS Site-to-Site VPN esistente.	• Sedi senza AWS Direct AWS Site-to-Site Connect/VPN. • Progetti sensibili ai costi.
Vantaggi principali	Vantaggi principali
• Connettività coerente a bassa latenza. • Allocazione dedicata della larghezza di banda. • Prestazioni di rete più affidabili. • La crittografia HCX predefinita può essere disabilitata per gli ambienti privati per ottimizzare le prestazioni. • Non è richiesta la gestione degli IP pubblici.	• Configurazione più rapida rispetto alla connettività privata. • Conveniente per le migrazioni più piccole.
Considerazioni chiave	Considerazioni chiave

Connettività privata	Connettività pubblica
• Configurazione iniziale più complessa. • Costi iniziali più elevati per l'infrastruttura. • Tempi di implementazione più lunghi. • Nessuna connettività Internet diretta per nessun componente HCX.	• Prestazioni di rete più variabili. • Sono possibili limitazioni della larghezza di banda. • Latenza più elevata rispetto alla connettività privata. • Ogni componente richiede un indirizzo IP elastico dedicato allocato dal pool IPAM pubblico. • Le associazioni EIP consentono la connettiv ità Internet diretta per ogni componente HCX.

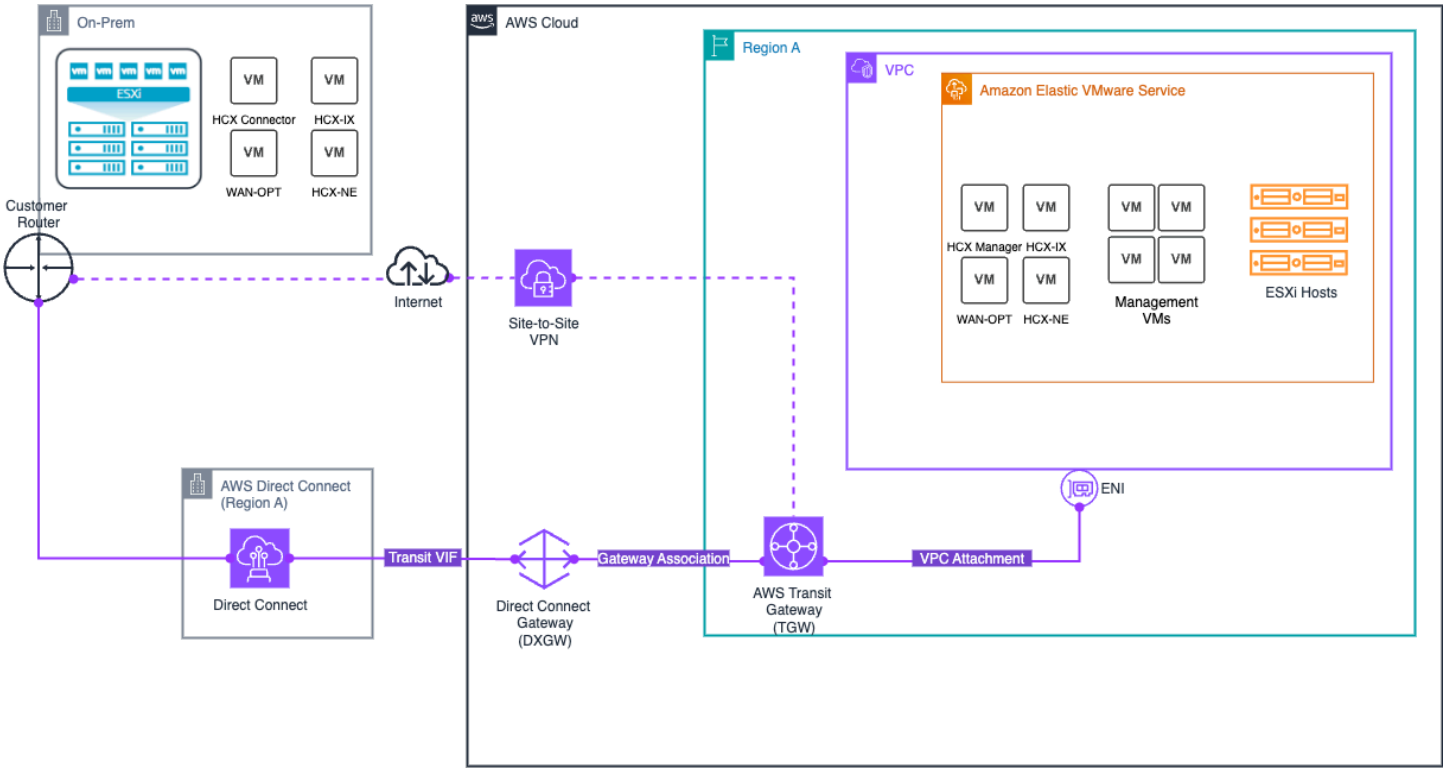
Architettura di connettività privata HCX

La soluzione di connettività privata HCX integra diversi componenti:

- Componenti di rete Amazon EVS
  - Utilizza solo sottoreti VLAN private per comunicazioni sicure, inclusa una VLAN HCX privata.
  - Supporta la rete per il controllo del traffico. ACLs
  - Supporta la propagazione dinamica BGP delle rotte tramite un server di routing VPC privato.
- AWS opzioni di transito di rete gestite per la connettività locale
  - AWS Direct Connect+ AWS Transit Gateway ti consente di connettere la tua rete locale ad Amazon EVS tramite una connessione privata dedicata. Per ulteriori informazioni, consulta AWS Direct Connect+ AWS Transit Gateway.
  - AWS Site-to-Site VPN+ AWS Transit Gateway offre la possibilità di creare una connessione IPsec VPN tra la rete remota e il gateway di transito su Internet. Per ulteriori informazioni, consulta AWS Transit Gateway + AWS Site-to-Site VPN.

> **Note**
>
> Amazon EVS non supporta la connettività tramite un'interfaccia virtuale privata (VIF) AWS Direct Connect o tramite una connessione AWS Site-to-Site VPN che termina direttamente nel VPC sottostante.

Il diagramma seguente illustra l'architettura di connettività privata HCX, mostrando come utilizzare AWS Direct Connect e Site-to-Site VPN con il gateway di transito per consentire la migrazione sicura del carico di lavoro tramite una connessione privata dedicata.



Architettura di connettività Internet HCX

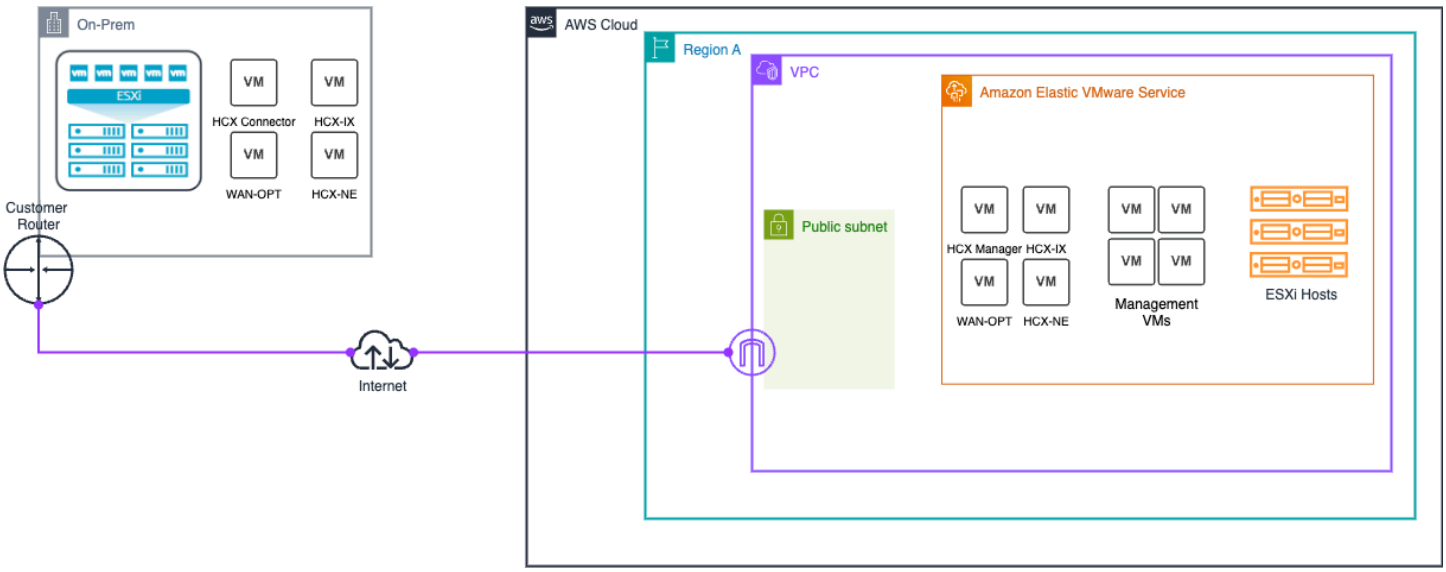
La soluzione di connettività Internet HCX è composta da diversi componenti che lavorano insieme:

- Componenti di rete Amazon EVS
  - Utilizza una sottorete VLAN HCX pubblica isolata per abilitare la connettività Internet tra Amazon EVS e i dispositivi HCX locali.
  - ACLs Supporta la rete per il controllo del traffico.
  - Supporta la propagazione dinamica BGP delle rotte attraverso un server di routing VPC pubblico.

- IPAM e gestione degli IP pubblici
  - Amazon VPC IP Address Manager (IPAM) gestisce l'allocazione degli IPv4 indirizzi pubblici dal pool IPAM pubblico di proprietà di Amazon.
  - Il blocco VPC CIDR secondario (/28) viene allocato dal pool IPAM, creando una sottorete pubblica isolata separata dal CIDR VPC principale.

Per ulteriori informazioni, consulta the section called "Connettività pubblica HCX".

Il diagramma seguente illustra l'architettura di connettività Internet HCX.



Configurazione della migrazione HCX

Questo tutorial descrive come configurare VMware HCX per migrare i carichi di lavoro su Amazon EVS.

Prerequisiti

Prima di utilizzare VMware HCX con Amazon EVS, assicurati che i prerequisiti HCX siano soddisfatti. Per ulteriori informazioni, consulta the section called "Prerequisiti per VMware HCX".

> **Important**
>
> Amazon EVS ha requisiti unici per la connettività Internet pubblica HCX.
> Se hai bisogno della connettività pubblica HCX, devi soddisfare i seguenti requisiti:

- Crea un IPAM e un pool IPv4 IPAM pubblico con CIDR con una lunghezza minima della maschera di rete di /28.
- Alloca almeno due indirizzi IP elastici (EIPs) dal pool IPAM per i dispositivi HCX Manager e HCX Interconnect (HCX-IX). Assegna un indirizzo IP elastico aggiuntivo per ogni appliance di rete HCX da distribuire.
- Aggiungi il blocco IPv4 CIDR pubblico come CIDR aggiuntivo al tuo VPC.

Per ulteriori informazioni, consulta the section called "Configurazione della connettività Internet HCX".

Controlla lo stato della sottorete VLAN HCX

Viene creata una VLAN per HCX come parte della distribuzione standard di Amazon EVS. Segui questi passaggi per verificare che la sottorete VLAN HCX sia configurata correttamente.

Example

Amazon EVS console

1. Vai alla console Amazon EVS.
2. Nel riquadro di navigazione, selezionare Compute environments (Ambienti di calcolo).
3. Seleziona l'ambiente Amazon EVS.
4. Seleziona la scheda Reti e connettività.
5. In VLANs, identifica la VLAN HCX e verifica che lo stato sia creato e pubblico sia vero.

AWS CLI

1. Esegui il comando seguente, utilizzando l'ID di ambiente per il tuo ambiente e il nome della regione che contiene le tue risorse.

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

2. Nell'output di risposta, identifica la VLAN con un `functionName` of `hcx` e verifica che `vlanState` `isPublic` sia `CREATED` impostato `true` su. Di seguito è riportata una risposta di esempio.


```
{
    "environmentVlans": [{
            "vlanId": 50,
            "cidr": "10.10.4.0/24",
            "availabilityZone": "us-east-2b",
            "functionName": "vTep",
            "subnetId": "subnet-0ce640ac79e7f4dbc",
            "createdAt": "2025-09-09T12:09:37.526000-07:00",
            "modifiedAt": "2025-09-09T12:35:00.596000-07:00",
            "vlanState": "CREATED",
            "stateDetails": "VLAN successfully created",
            "eipAssociations": [],
            "isPublic": false
        },
        {
            "vlanId": 80,
            "cidr": "18.97.141.240/28",
            "availabilityZone": "us-east-2b",
            "functionName": "hcx",
            "subnetId": "subnet-0f080c94782cc74b4",
            "createdAt": "2025-09-09T12:09:37.675000-07:00",
            "modifiedAt": "2025-09-09T12:35:00.359000-07:00",
            "vlanState": "CREATED",
            "stateDetails": "VLAN successfully created",
            "eipAssociations": [{
                    "assocationId": "eipassoc-0be981accbbdf443a",
                    "allocationId": "eipalloc-0cef80396f4a0cc24",
                    "ipAddress": "18.97.141.245"
                },
                {
                    "assocationId": "eipassoc-0d5572f66b7952e9d",
                    "allocationId": "eipalloc-003fc9807d35d1ad3",
                    "ipAddress": "18.97.141.244"
                }
            ],
            "isPublic": true
        }
    ]
```

```
}
```

Verificate che la sottorete VLAN HCX sia associata a un ACL di rete

Segui questi passaggi per verificare che la sottorete VLAN HCX sia associata a un ACL di rete. Per ulteriori informazioni sull'associazione ACL di rete, vedere. the section called "Crea un ACL di rete per controllare il traffico della sottorete VLAN di Amazon EVS"

> **Important**
>
> Se ti connetti tramite Internet, l'associazione di un indirizzo IP elastico a una VLAN fornisce l'accesso diretto a Internet a tutte le risorse su quella VLAN. Assicurati di disporre di elenchi di controllo degli accessi alla rete configurati in modo da limitare l'accesso in base alle esigenze di sicurezza.

> **Important**
>
> EC2 i gruppi di sicurezza non funzionano su interfacce di rete elastiche collegate alle sottoreti VLAN di Amazon EVS. Per controllare il traffico da e verso le sottoreti VLAN di Amazon EVS, devi utilizzare una lista di controllo degli accessi alla rete (ACL).

Example

Amazon VPC console

1. Vai alla console. Amazon VPC
2. Nel pannello di navigazione, scegli Rete ACLs.
3. Seleziona l'ACL di rete a cui sono associate le sottoreti VLAN.
4. Seleziona la scheda Associazioni delle sottoreti.
5. Verificate che la sottorete VLAN HCX sia elencata tra le sottoreti associate.

AWS CLI

1. Esegui il comando seguente, utilizzando l'ID di sottorete VLAN HCX nel filtro. `Values`

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

2. Verificare che nella risposta venga restituito l'ACL di rete corretto.

Verifica che le sottoreti VLAN EVS siano associate esplicitamente a una tabella di routing

Amazon EVS richiede che tutte le sottoreti VLAN EVS siano associate esplicitamente a una tabella di routing nel tuo VPC. Per la connettività Internet HCX, la sottorete VLAN pubblica HCX deve essere associata in modo esplicito a una tabella di routing pubblica nel VPC che indirizza verso un gateway Internet. Segui questi passaggi per verificare l'associazione esplicita della tabella di routing.

Example

Amazon VPC console

1. Vai alla console VPC.
2. Nel riquadro di navigazione, seleziona Tabelle di routing.
3. Scegli la tabella di routing a cui le tue sottoreti VLAN EVS devono essere associate in modo esplicito.
4. Seleziona la scheda Associazioni delle sottoreti.
5. In Associazioni di sottoreti esplicite, verifica che tutte le sottoreti EVS VLAN siano elencate. Se una sottorete VLAN non è elencata qui, la sottorete VLAN è associata implicitamente alla tabella di routing principale. Affinché Amazon EVS funzioni correttamente, è necessario associare esplicitamente tutte le sottoreti VLAN a una tabella di routing. Per la sottorete VLAN pubblica HCX, è necessario disporre di una tabella di routing pubblica associata con un gateway Internet come destinazione. Per risolvere questo problema, scegli Modifica associazioni di sottoreti e aggiungi le sottoreti VLAN mancanti.

AWS CLI

1. Apri una sessione terminale.
2. Esegui il seguente comando di esempio per recuperare i dettagli su tutte le sottoreti VLAN EVS, inclusa l'associazione delle tabelle di routing. Se una sottorete VLAN non è elencata qui,

la sottorete VLAN viene associata implicitamente alla tabella di routing principale. Affinché Amazon EVS funzioni correttamente, è necessario associare esplicitamente tutte le sottoreti VLAN a una tabella di routing. Per la sottorete VLAN pubblica HCX, è necessario disporre di una tabella di routing pubblica associata con un gateway Internet come destinazione.

```
aws ec2 describe-subnets
```

3. Associa esplicitamente le sottoreti VLAN EVS a una tabella di routing nel tuo VPC. Di seguito è riportato un comando di esempio.

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

(Per la connettività Internet HCX) Verifica che EIPs siano associati alla sottorete VLAN HCX

Per ogni appliance di rete HCX da distribuire, è necessario disporre di un EIP proveniente dal pool IPAM associato a una sottorete VLAN pubblica HCX. È necessario associarne almeno due EIPs alla sottorete VLAN pubblica HCX per i dispositivi HCX Manager e HCX Interconnect (HCX-IX). Segui questi passaggi per verificare che esistano le associazioni EIP necessarie.

Important

La connettività Internet pubblica HCX non riesce se non si associano almeno due del pool IPAM a una EIPs sottorete VLAN pubblica HCX.

Note

Non è possibile associare i primi due EIPs o gli ultimi EIP del blocco CIDR IPAM pubblico a una sottorete VLAN. Questi EIPs sono riservati come indirizzi di rete, gateway predefiniti e indirizzi di trasmissione. Amazon EVS genera un errore di convalida se tenti di EIPs associarli a una sottorete VLAN.

Example

Amazon EVS console

1. Vai alla console Amazon EVS.
2. Nel menu di navigazione, scegli Ambienti.
3. Seleziona l'ambiente.
4. Nella scheda Reti e connettività, seleziona la VLAN pubblica HCX.
5. Controlla la scheda delle associazioni EIP per confermare che siano EIPs state associate alla VLAN pubblica HCX.

AWS CLI

1. Per verificare quali EIPs sono associati alla sottorete VLAN HCX, utilizzare il comando. `list-environment-vlans` Per`environment-id`, usa l'ID univoco per l'ambiente EVS che contiene la VLAN HCX.

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

Il comando restituisce dettagli sulle tue associazioni VLANs, incluse le tue associazioni EIP:


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

```
        },
        {
          "associationId": "eipassoc-12345678901abcdef",
          "allocationId": "eipalloc-1234567890abcdef1",
          "ipAddress": "18.97.137.4"
        },
        {
          "associationId": "eipassoc-23456789012abcdef",
          "allocationId": "eipalloc-2345678901abcdef2",
          "ipAddress": "18.97.137.5"
        }
      ],
      "isPublic": true,
      "networkAclId": "acl-0123456789abcdef0"
    },
    ...
  ]
}
```

L'`eipAssociations`array mostra l'associazione EIP, tra cui:

- `associationId`- L'ID univoco per questa associazione EIP.
- `allocationId`- L'ID di allocazione dell'indirizzo IP elastico associato.
- `ipAddress`- L'indirizzo IP assegnato alla VLAN.

Crea un gruppo di porte distribuito con l'ID VLAN uplink pubblico HCX

Accedere all'interfaccia di vSphere Client e seguire i passaggi in Aggiungi un gruppo di porte distribuite per aggiungere un gruppo di porte distribuito a un vSphere Distributed Switch.

Quando si configura il failback all'interno dell'interfaccia vSphere Client, assicurarsi che uplink1 sia un uplink attivo e uplink2 sia un uplink in standby per abilitare il failover. Active/Standby Per l'impostazione VLAN nell'interfaccia vSphere Client, immettere l'ID VLAN HCX identificato in precedenza.

(Facoltativo) Configurare l'ottimizzazione della rete WAN HCX

> **Note**
>
> La funzionalità di ottimizzazione WAN non è più disponibile in HCX 4.11.3. Per ulteriori informazioni, consulta le note di rilascio di HCX 4.11.3.

Il servizio HCX WAN Optimization (HCX-WO) migliora le caratteristiche prestazionali delle linee private o dei percorsi Internet applicando tecniche di ottimizzazione WAN come la riduzione dei dati e il condizionamento dei percorsi WAN. Il servizio HCX WAN Optimization è consigliato nelle implementazioni che non sono in grado di dedicare percorsi da 10 Gbit per le migrazioni. Nelle implementazioni da 10 Gbit a bassa latenza, l'utilizzo di WAN Optimization potrebbe non consentire di migliorare le prestazioni di migrazione. Per ulteriori informazioni, consulta Considerazioni e best practice sull'implementazione di VMware HCX.

Il servizio HCX WAN Optimization viene distribuito insieme all'appliance del servizio HCX WAN Interconnect (HCX-IX). HCX-IX è responsabile della replica dei dati tra l'ambiente aziendale e l'ambiente Amazon EVS.

Per utilizzare il servizio HCX WAN Optimization con Amazon EVS, è necessario utilizzare un gruppo di porte distribuito sulla sottorete VLAN HCX. Utilizza il gruppo di porte distribuito creato nel passaggio precedente.

(Facoltativo) Abilita la rete ottimizzata per la mobilità HCX

HCX Mobility Optimized Networking (MON) è una funzionalità dell'HCX Network Extension Service. Le estensioni di rete abilitate al MON migliorano i flussi di traffico per le macchine virtuali migrate abilitando il routing selettivo all'interno del tuo ambiente Amazon EVS. MON consente di configurare il percorso ottimale per la migrazione del traffico del carico di lavoro verso Amazon EVS quando si estendono reti di livello 2, evitando un lungo percorso di rete di andata e ritorno attraverso il gateway di origine. Questa funzionalità è disponibile per tutte le implementazioni di Amazon EVS. Per ulteriori informazioni, consulta Configurazione della rete ottimizzata per la mobilità nella Guida per l' VMware utente di HCX.

> **Important**
>
> Prima di abilitare HCX MON, leggi le seguenti limitazioni e configurazioni non supportate per HCX Network Extension.

Restrizioni e limitazioni per l'estensione di rete
Restrizioni e limitazioni per topologie di rete ottimizzate per la mobilità

Important

Prima di abilitare HCX MON, assicurati di aver configurato la ridistribuzione del percorso per il CIDR della rete di destinazione nell'interfaccia NSX. Per ulteriori informazioni, consulta Configurare BGP e la ridistribuzione del percorso nella documentazione di NSX. VMware

Verifica la connettività HCX

VMware HCX include strumenti diagnostici integrati che possono essere utilizzati per testare la connettività. Per ulteriori informazioni, vedere Risoluzione dei problemi VMware HCX nella Guida per l'VMware utente di HCX.

Configurazione della connettività Internet pubblica HCX

Puoi configurare l'accesso pubblico a Internet per la tua VLAN pubblica HCX associando indirizzi IP elastici alla tua VLAN. Ciò consente la connettività Internet diretta per i dispositivi e i carichi di lavoro VMware HCX che richiedono l'accesso a Internet per le operazioni di migrazione.

Argomenti correlati

Questo argomento tratta la gestione dell'accesso a Internet per la VLAN pubblica HCX. Per un'implementazione completa:

1. Completa i prerequisiti inConfigurazione di Amazon Elastic VMware Service.
2. Configurare la configurazione iniziale inNozioni di base.
3. Configurare l'accesso a Internet (questo argomento).

Informazioni sull'accesso a Internet tramite VLAN HCX

Puoi configurare l'accesso a Internet per le appliance VMware HCX, consentendoti di eseguire la migrazione HCX dei tuoi carichi di lavoro su Amazon EVS tramite Internet.

Questo approccio:

- Consente la migrazione delle macchine virtuali senza richiedere una connettività privata dedicata.
- Fornisce una soluzione flessibile ed economica per la migrazione.

> **Important**
>
> La migrazione HCX basata su Internet in genere non è consigliata per:
>
> - Applicazioni sensibili al jitter o alla latenza della rete.
> - Operazioni vMotion critiche in termini di tempo.
> - Migrazioni su larga scala con requisiti prestazionali rigorosi.
>
> Per questi scenari, consigliamo di utilizzare la connettività privata HCX. Una connessione privata dedicata offre prestazioni più affidabili rispetto alle connessioni basate su Internet.

Panoramica della connettività Internet

Esamina le seguenti considerazioni.

Requisiti di rete HCX e DNAT

HCX presenta vincoli di rete specifici che influiscono sulla configurazione dell'accesso pubblico a Internet.

HCX non supporta DNAT (Destination Network Address Translation). HCX richiede invece che la rete uplink sia instradabile con un indirizzo IP gateway predefinito.

Le sottoreti VLAN di Amazon EVS includono un indirizzo IP gateway predefinito come le altre sottoreti VPC. Tuttavia, queste sottoreti sono sempre sottoreti private, anche quando si utilizzano blocchi CIDR al di fuori dell'intervallo di indirizzi. RFC1918

Abilitazione della connettività Internet HCX

Per abilitare la connettività Internet senza DNAT, Amazon EVS utilizza un approccio di configurazione CIDR specifico:

- Requisito CIDR instradabile su Internet: Amazon EVS richiede un CIDR instradabile su Internet che corrisponda al CIDR della sottorete VLAN HCX.

- Allocazione IPAM: Amazon EVS utilizza un CIDR pubblico allocato tramite IPAM con una lunghezza minima della maschera di rete di /28 come CIDR instradabile su Internet.
- Configurazione VPC: devi aggiungere manualmente il CIDR pubblico allocato da IPAM al tuo VPC come CIDR VPC secondario.
- Distribuzione di sottoreti VLAN: dopo aver configurato IPAM e VPC, puoi utilizzare il CIDR pubblico allocato da IPAM nella sottorete VLAN HCX durante la distribuzione di Amazon EVS.
- Configurazione IP elastica: Amazon EVS richiede la seguente configurazione:
  - Allocazione elastica IPs: si alloca Elastic IPs dal CIDR allocato in IPAM. È necessario allocare almeno due indirizzi IP elastici (EIPs) dal pool IPAM per le appliance HCX Manager e HCX Interconnect (HCX-IX). Assegna un indirizzo IP elastico aggiuntivo per ogni appliance di rete HCX da distribuire.
  - Associa a VLAN: associ ogni IP elastico che desideri utilizzare con un'appliance HCX alla sottorete VLAN HCX. Usa la console Amazon EVS o AWS CLI per questa associazione.
  - Configura l'indirizzo del gateway: il primo indirizzo utilizzabile del CIDR diventa l'indirizzo gateway che configuri nel tuo dispositivo HCX.
  - Routing del traffico: il traffico per ogni IP elastico associato viene indirizzato direttamente all'appliance HCX di destinazione con lo stesso indirizzo IP, senza DNAT.

Per i passaggi per configurare HCX con connettività Internet per la distribuzione dell'ambiente Amazon EVS, consulta e. Configurazione di Amazon Elastic VMware Service Nozioni di base

Considerazioni operative

- Il blocco CIDR VLAN pubblico HCX deve avere una lunghezza della netmask /28.
- EIPs possono essere associati o dissociati dalla VLAN pubblica HCX dopo la distribuzione utilizzando la console Amazon EVS oppure AWS CLI, ma devono provenire dallo stesso pool IPAM.
- Ogni associazione EIP ha il proprio ID di associazione univoco.
- È possibile avere fino a 13 EIPs da un pool IPAM pubblico associato alla VLAN pubblica /28 HCX. Non è possibile associare i primi due EIPs o gli ultimi EIP del blocco CIDR pubblico allocato da IPAM alla sottorete VLAN pubblica HCX. Questi EIPs sono riservati come indirizzi di rete, gateway predefiniti e indirizzi di trasmissione. Amazon EVS genera un errore di convalida se tenti di EIPs associarli alla VLAN.

Considerazioni relative alla sicurezza

- Le liste di controllo dell'accesso alla rete (ACLs) si applicano ancora al traffico che scorre attraverso la sottorete VLAN pubblica HCX.
- Le regole dei gruppi di sicurezza non si applicano al traffico sulle sottoreti VLAN pubbliche HCX. Usa la rete per il controllo del traffico. ACLs

> **Important**
>
> Se ti connetti tramite Internet, l'associazione di un indirizzo IP elastico a una VLAN fornisce l'accesso diretto a Internet a tutte le risorse su quella VLAN. Assicurati di disporre di elenchi di controllo degli accessi alla rete configurati in modo da limitare l'accesso in base alle esigenze di sicurezza.

Gestione degli indirizzi IP elastici per VLANs

Puoi associare e dissociare gli indirizzi IP elastici con una VLAN pubblica HCX utilizzando la console Amazon EVS o. AWS CLI

> **Note**
>
> Al momento Amazon EVS supporta solo l'associazione e la dissociazione dell'indirizzo IP elastico con una VLAN pubblica HCX.

Associa un indirizzo IP elastico a una VLAN

Prerequisiti

Assicurati di disporre di quanto segue:

- L'indirizzo IP elastico viene allocato dal pool IPAM pubblico di proprietà di Amazon.
- L'ambiente Amazon EVS è già stato creato.

Example

Amazon EVS console

1. Vai alla console Amazon EVS.
2. Nel menu di navigazione, scegli Ambienti.
3. Seleziona l'ambiente.
4. Nella scheda Reti e connettività, seleziona la VLAN pubblica HCX.

> **Note**
>
> Al momento Amazon EVS supporta solo l'associazione EIPs alla VLAN HCX.

5. Scegli Associa EIP a VLAN.
6. Seleziona gli indirizzi IP elastici da associare alla VLAN pubblica HCX.
7. Selezionare Associate (Associa) EIPs. È possibile avere fino a 13 EIPs associati alla VLAN pubblica HCX.

> **Note**
>
> Non è possibile associare i primi due EIPs dal blocco CIDR IPAM pubblico alla sottorete VLAN. Questi EIPs sono riservati come indirizzi di rete e gateway predefiniti.

8. Controlla le associazioni EIP per confermare che siano EIPs state associate alla VLAN pubblica HCX.

AWS CLI

1. Per associare un indirizzo IP elastico a una VLAN, usa il comando example. `associate-eip-to-vlan`
   - `environment-id`- L'ID del tuo ambiente Amazon EVS.
   - `vlan-name`- Deve esserlo. `hcx` Al momento Amazon EVS supporta solo l'associazione EIP con la VLAN HCX.
   - `allocation-id`- L'ID di allocazione dell'indirizzo IP elastico.

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

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

Il comando restituisce dettagli sulla VLAN, inclusa la nuova associazione EIP:


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


L'`eipAssociations`array mostra la nuova associazione, tra cui:

- `associationId`- L'ID univoco di questa associazione EIP, utilizzato per la dissociazione.
- `allocationId`- L'ID di allocazione dell'indirizzo IP elastico associato.
- `ipAddress`- L'indirizzo IP assegnato alla VLAN.

2. Ripetere il passaggio per associarne altri EIPs. È possibile EIPs associarne fino a 13 alla VLAN pubblica HCX.

Dissocia un indirizzo IP elastico da una VLAN

Prerequisiti

Assicurati di disporre di quanto segue:

- L'ambiente Amazon EVS è già stato creato.
- EIP è associato all'ambiente Amazon EVS.

Example

Amazon EVS console

1. Vai alla console Amazon EVS.
2. Nel menu di navigazione, scegli Ambienti.
3. Seleziona l'ambiente.
4. Nella scheda Reti e connettività, seleziona la VLAN pubblica HCX.
5. Scegli Dissocia EIP da VLAN.
6. Seleziona gli indirizzi IP elastici da dissociare dalla VLAN pubblica HCX.

> **Important**
>
> La dissociazione EIPs può causare una perdita di connettività Internet per i dispositivi che utilizzano sottoreti VLAN pubbliche.

7. Scegli Dissocia EIPs.
8. Controlla le associazioni EIP per confermare che EIPs sono state dissociate dalla VLAN pubblica HCX.

AWS CLI

Per dissociare un indirizzo IP elastico da una VLAN, usa il comando example. `disassociate-eip-from-vlan`

- `environment-id`- L'ID del tuo ambiente Amazon EVS.
- `vlan-name`- Deve esserlo. `hcx` Al momento Amazon EVS supporta solo l'associazione EIP con la VLAN HCX.
- `association-id`- L'ID dell'associazione EIP da rimuovere.

> **Important**
>
> La dissociazione EIPs può causare una perdita di connettività Internet per i dispositivi che utilizzano sottoreti VLAN pubbliche.

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

Il comando restituisce i dettagli sulla VLAN con l'associazione EIP rimossa:

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

L'`eipAssociations`array vuoto conferma che l'indirizzo IP elastico è stato correttamente dissociato dalla VLAN.

Informazioni sull'ottimizzazione della rete WAN HCX per le migrazioni basate su Internet

> **Note**
>
> La funzionalità di ottimizzazione WAN non è più disponibile in HCX 4.11.3. Per ulteriori informazioni, consulta le note di rilascio di HCX 4.11.3.

Quando si eseguono migrazioni su Internet, HCX WAN Optimization (HCX-WO) può migliorare le prestazioni di migrazione. Il servizio funziona in combinazione con l'appliance HCX Interconnect (HCX-IX) per:

- Applica tecniche di riduzione dei dati per ridurre al minimo l'utilizzo della larghezza di banda.
- Implementa il condizionamento dei percorsi WAN per ottimizzare le prestazioni di rete.
- Migliora la velocità di migrazione su connessioni Internet ad alta latenza.
- Migliora l'affidabilità delle migrazioni basate su Internet.

L'ottimizzazione della rete WAN HCX è particolarmente utile per le migrazioni basate su Internet in cui:

- La latenza di rete può essere superiore rispetto alle opzioni di connettività privata.
- La larghezza di banda disponibile può essere limitata o variabile.
- Le condizioni della rete possono variare a causa dei modelli di traffico Internet.

Per istruzioni dettagliate sulla configurazione di HCX WAN Optimization dopo la configurazione della connettività Internet, vedere. the section called "(Facoltativo) Configurare l'ottimizzazione della rete WAN HCX"

> **Note**
>
> Sebbene l'ottimizzazione della WAN possa migliorare in modo significativo le prestazioni di migrazione basata su Internet, potrebbe non offrire vantaggi aggiuntivi in ambienti con connessioni dedicate da 10 Gbit a bassa latenza. Considerate le caratteristiche della rete quando decidete se abilitare questa funzionalità.

Gestione degli ambienti Amazon EVS

Questo capitolo include i seguenti argomenti per aiutarti a gestire il tuo ambiente.

- the section called "Abbonamenti VCF"- Descrive come funzionano gli abbonamenti VCF con Amazon EVS e le responsabilità dei clienti per la gestione degli abbonamenti VCF.
- the section called "Versioni VCF e istanze EC2"- Descrive le versioni VCF ed ESX supportate e come verificare la disponibilità delle versioni in Amazon EVS.
- the section called "Gestione del ciclo di vita"- Descrive le responsabilità di gestione del ciclo di vita all'interno di un ambiente Amazon EVS, inclusa la gestione dell'infrastruttura sottostante, la gestione degli upgrade VCF, la gestione del ciclo di vita dell'host ESX.
- the section called "Manutenzione dell'ambiente"- Descrive come eseguire attività di manutenzione comuni per il tuo ambiente Amazon EVS, tra cui configurazione di rete, manutenzione dell'host ESX, controllo dello stato dell'ambiente e gestione di pianificazioni di rotazione segrete per le tue credenziali VCF.
- the section called "Crea host"- Descrive come creare un host Amazon EVS dopo la distribuzione dell'ambiente e aggiungere l'host al cluster.
- the section called "Eliminare un host"- Descrive come eliminare un host Amazon EVS e rimuoverlo dal cluster.
- the section called "Crea connettore"- Descrive come creare un connettore di ambiente Amazon EVS per stabilire una connessione persistente tra Amazon EVS e un'appliance VCF.
- the section called "Aggiorna connettore"- Descrive come aggiornare un connettore di ambiente Amazon EVS per modificare il nome di dominio completo dell'appliance o il segreto di Secrets Manager.
- the section called "Elimina connettore"- Descrive come eliminare un connettore di ambiente Amazon EVS.
- the section called "Crea un'autorizzazione"- Descrive come creare un'autorizzazione Amazon EVS per abilitare la copertura delle licenze Windows AWS offerta per le macchine virtuali.
- the section called "Eliminare l'autorizzazione"- Descrive come eliminare l'autorizzazione Amazon EVS a rimuovere la copertura delle licenze Windows AWS offerta dalle macchine virtuali.
- the section called "Configurare l'attivazione di Windows Server"- Descrive come configurare l'attivazione di Windows Server su macchine virtuali con autorizzazioni Windows Server.
- the section called "Depot Addon personalizzato"- Descrive come accedere al depot Amazon EVS Custom Addon e configurarlo come sorgente di download in vLCM.

Abbonamenti VCF

> **Note**
>
> Amazon EVS non supporta licenze vSphere perpetue. È necessario disporre di un abbonamento VMware Cloud Foundation valido e attivo per utilizzare Amazon EVS.

Amazon EVS utilizza gli abbonamenti VMware Cloud Foundation (VCF) con diritti di portabilità delle licenze che offri a (BYOS). AWS Per implementare correttamente un ambiente Amazon EVS, devi fornire una chiave di soluzione VCF valida e una chiave di licenza vSAN nella richiesta di creazione dell'ambiente. La chiave di licenza vSphere funge da chiave di soluzione per VCF. Ogni chiave di licenza VCF può essere utilizzata per un solo ambiente Amazon EVS. La creazione dell'ambiente non riesce se si tenta di utilizzare una chiave di licenza VCF già utilizzata in un altro ambiente.

La chiave della soluzione VCF deve avere core sufficienti per fornire una capacità core adeguata per i quattro host EC2 iniziali che Amazon EVS distribuisce al momento della creazione dell'ambiente. Il numero di core richiesto dipende dal tipo di istanza selezionato, poiché ogni tipo di istanza ha un numero diverso di core.

Tipo di istanza	Core per host	Numero minimo di core per 4 host (licenza VCF)
i4i.metal	64	256
i7i.metal-24xl	48	192

La chiave di licenza vSAN deve soddisfare i requisiti di instance-type-specific capacità. La capacità richiesta dipende dal tipo di istanza selezionato:

Tipo di istanza	Capacità vSAN minima per 4 host (licenza vSAN)
i4i.metal	110 TiB
i7i.metal-24xl	82 TiB

La creazione dell'ambiente fallisce se si tenta di utilizzare chiavi di licenza sottodimensionate.

> **Note**
>
> Il tuo abbonamento VCF sarà disponibile per Amazon EVS in tutte le AWS regioni per la conformità delle licenze. Amazon EVS non convalida le chiavi di licenza. Per convalidare le chiavi di licenza, visita l'assistenza Broadcom.

> **Note**
>
> Le informazioni sul tuo software VCF in Amazon EVS verranno condivise con Broadcom per verificare la conformità della licenza.

Gestione delle sottoscrizioni

Sei responsabile della gestione dei tuoi abbonamenti VCF. Gli abbonamenti VCF devono essere gestiti in SDDC Manager. La rimozione delle chiavi di licenza da SDDC Manager o la loro sostituzione con una chiave di licenza in uso comporterà un errore nel controllo dello stato dell'ambiente, che ti impedirà di aggiungere host al tuo ambiente Amazon EVS. Per ulteriori informazioni sui controlli dello stato dell'ambiente, e. the section called “Monitora lo stato dell'ambiente” the section called “Risolvi i problemi relativi ai controlli dello stato dell'ambiente non riusciti” Per ulteriori informazioni sulle chiavi di licenza VCF, consulta Gestione delle chiavi di licenza in VMware Cloud Foundation nella documentazione di VMware Cloud Foundation.

> **Important**
>
> Utilizza l'interfaccia utente SDDC Manager per gestire la soluzione VCF e le chiavi di licenza vSAN. Amazon EVS richiede il mantenimento di una soluzione VCF valida e delle chiavi di licenza vSAN in SDDC Manager per il corretto funzionamento del servizio. Sebbene le chiavi debbano essere assegnate agli host e al cluster vSAN utilizzando vSphere Client, è necessario assicurarsi che tali chiavi vengano visualizzate anche nella schermata delle licenze dell'interfaccia utente di SDDC Manager.

Aggiungere le chiavi di licenza VCF

Nel portale di supporto Broadcom, puoi acquistare chiavi di licenza VCF aggiuntive, dividere chiavi di licenza se disponi già di chiavi di grandi dimensioni o unire più chiavi di licenza. Ciò consente di concedere in licenza gli host aggiunti all'ambiente dopo la distribuzione iniziale o concedere in licenza ambienti aggiuntivi. Assicurati che le chiavi di licenza acquistate vengano aggiunte all'inventario di vCenter Server e SDDC Manager. Se aggiungi host, assicurati che le licenze siano assegnate agli host corretti in vSphere e che dispongano di core e capacità di storage vSAN adeguati. Amazon EVS non supporta host senza licenza. Per ulteriori informazioni, vedere Configurazione delle impostazioni di licenza per gli asset nel client vSphere nella VMware documentazione.

Le nuove chiavi di licenza non scadute devono essere assegnate a vCenter Server prima della scadenza del periodo di valutazione della chiave di licenza per rimanere attive. Le chiavi di licenza attive sono necessarie per configurare correttamente un ambiente Amazon EVS. L'ambiente non verrà distribuito se viene fornita una chiave di licenza scaduta. Per ulteriori informazioni sulla creazione della chiave di licenza VCF, consulta Creare una nuova licenza nella documentazione. VMware Se riscontri problemi con le chiavi di licenza aggiunte, consultathe section called "Controllo della copertura delle chiavi non riuscito".

Rimozione delle chiavi di licenza VCF

È possibile rimuovere le chiavi di licenza VCF dall'inventario di SDDC Manager per ridurre la capacità principale e vSAN dopo l'eliminazione degli host nell'ambiente. Per rimanere conformi ai modelli di licenza dei prodotti utilizzati con vSphere, è necessario rimuovere tutte le chiavi di licenza non assegnate dall'inventario. Se nel Broadcom Support Portal sono presenti chiavi di licenza divise, unite o aggiornate, è necessario rimuovere le vecchie chiavi di licenza. Per ulteriori informazioni, consulta Rimuovere una licenza nella documentazione. VMware

Versioni VCF e tipi di istanze EC2 forniti da Amazon EVS

Amazon EVS offre diverse versioni dei tipi di istanze VMware Cloud Foundation (VCF), ESX ed EC2 che puoi selezionare durante la creazione di un ambiente e di un host.

Verifica delle versioni VCF fornite, delle versioni ESX e dei tipi di istanze EC2

La AWS console mostra l'elenco delle versioni VCF fornite da Amazon EVS nella procedura guidata di creazione dell'ambiente. Le versioni ESX disponibili sono visibili quando si seleziona un tipo di

istanza durante l'aggiunta di un host a un ambiente esistente. Puoi anche visualizzare le versioni VCF, le versioni ESX e i tipi di istanze EC2 utilizzando la CLI.

Example

Amazon EVS console

1. Vai alla console Amazon EVS.
2. Nel menu di navigazione, scegli Ambienti.
3. Esegui una delle seguenti operazioni:

   Per controllare le versioni VCF:

   a. Seleziona Crea ambiente.
   b. In base ai requisiti di convalida di Amazon EVS, scegli la tua versione VCF per vedere se lo stato è disponibile o limitato per te.

   Per verificare le versioni ESX:

   a. Seleziona un ambiente esistente.
   b. Scegli Create host (Crea host).
   c. Seleziona un tipo di istanza per visualizzare le versioni ESX disponibili.

AWS CLI

Esegui il comando seguente per recuperare informazioni sulle versioni VCF ed ESX:

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

Risposta di esempio:

```
{
    "vcfVersions": [
        {
            "vcfVersion": "VCF-5.2.1",
            "status": "RESTRICTED",
            "defaultEsxVersion": "ESXi-8.0U3b-24280767",
            "instanceTypes": [
                "i4i.metal",
                "i7i.metal-24xl"
```

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

> **Note**
>
> Se la versione di cui hai bisogno `RESTRICTED` è disponibile e hai un'esigenza particolare, consulta the section called "Richiesta di accesso a versioni VCF con restrizioni" per ulteriori informazioni su come accedere a quella versione.

Versioni VCF attuali in Amazon EVS

Amazon EVS attualmente fornisce le seguenti versioni VCF per la creazione di ambienti:

Versione VCF	Versione ESX predefinita	Stato	Tipi di istanza EC2
VCF-5.2.2	ESXi-8,0u3G-24859861	DISPONIBILE	i4i.metal, i7i.metal-24xl
VCF-5.2.1	ESXi-8,0u3B-24280767	RISTRETTO	i4i.metal, i7i.metal-24xl

> **Note**
>
> Quando crei un nuovo ambiente Amazon EVS, devi specificare una versione VCF.

Considerazioni sulla versione ESX

Ogni versione VCF ha una versione ESX predefinita basata sulla distinta dei materiali (BOM) di Broadcom VCF. Quando si crea un nuovo ambiente, non è possibile scegliere una versione ESX specifica. La versione ESX predefinita per la versione VCF selezionata viene applicata automaticamente.

Tuttavia, quando si aggiunge un host all'ambiente, è possibile selezionare una versione ESX disponibile per il tipo di istanza scelto. Se non ne specifichi uno, Amazon EVS utilizza la versione ESX predefinita associata alla versione VCF del tuo ambiente.

Dopo l'aggiunta di un host, la sua versione ESX può essere aggiornata solo utilizzando vCenter Lifecycle Manager.

> **Note**
>
> Amazon EVS non fornisce tutte le versioni di VCF ed ESX rilasciate da Broadcom. Per informazioni sull'interoperabilità del software, consulta la Broadcom Interoperability Matrix. Per la piena compatibilità hardware con le istanze AWS EC2, consulta la Broadcom Compatibility Guide.

Richiesta di accesso a versioni VCF con restrizioni

Se hai bisogno di accedere a una versione VCF con uno `RESTRICTED` stato, contatta il AWS Supporto con le seguenti informazioni:

- L'ID del tuo AWS account
- La AWS regione
- La versione VCF specifica di cui hai bisogno
- Il tuo caso d'uso e la giustificazione aziendale (ad esempiosecurity/compliance, compatibility/dependency, e altri)

AWS L'assistenza esaminerà la tua richiesta e approverà o richiederà informazioni aggiuntive. Dopo l'approvazione, lo stato della versione verrà modificato `AVAILABLE` nella risposta della AWS console o dell'`get-versions`API.

Gestione del ciclo di vita dell'ambiente Amazon EVS

Questa pagina descrive le tue responsabilità di gestione del ciclo di vita all'interno di un ambiente Amazon EVS.

Uno dei vantaggi principali di Amazon EVS è che hai il controllo completo sulla tua VMware architettura nel cloud. Puoi ottimizzare lo stack software VMware Cloud Foundation (VCF) per soddisfare le esigenze specifiche delle tue applicazioni. Poiché Amazon EVS è un servizio autogestito, sei responsabile della gestione del ciclo di vita e della manutenzione del VMware software utilizzato nell'ambiente Amazon EVS, come ESX, vSphere, vSAN, NSX e SDDC Manager. Sei inoltre responsabile della manutenzione di eventuali integrazioni di terze parti, come le soluzioni di protezione dei dati che integri nei tuoi host Amazon EVS.

Sei responsabile della configurazione dei componenti di AWS rete sottostanti utilizzati da Amazon EVS, tra cui tabelle di routing VPC, gruppi di sicurezza e regole ACL (Network Access Control List), configurazione VPC Route Server, gateway Internet, gateway NAT e gateway di transito (per la connettività locale).

AWS è responsabile della distribuzione dell'ambiente Amazon EVS con le configurazioni di rete fornite dall'utente. La distribuzione dell'ambiente include quanto segue:

- Avvio della configurazione di rete del tuo ambiente Amazon EVS.
- Abilitazione del routing nord-sud con l'istanza del VPC Route Server fornita.

- Implementazione delle sottoreti VLAN EVS richieste, delle interfacce di rete elastiche e di quattro host ESX iniziali.
- Configurazione di una rete overlay NSX con un gateway Tier-0 e un gateway Tier-1.
- Implementazione di un cluster NSX Edge con due nodi NSX Edge in modalità. Active/Standby
- Creazione e configurazione del cluster vSAN iniziale e montaggio del datastore.

Sei responsabile della configurazione di VMware NSX, inclusi i segmenti di rete, le regole firewall distribuite e i sistemi di bilanciamento del carico. Sei anche responsabile della configurazione di tutte le soluzioni integrate che implementi con Amazon EVS dopo la distribuzione dell'ambiente EVS, inclusa la configurazione VMware HCX e i gateway NSX Tier-1 aggiuntivi.

Per ulteriori informazioni sulle responsabilità dei clienti, consulta il modello di responsabilità condivisa AWS .AWS

> **Note**
>
> Un gateway Tier-0 e un gateway Tier-1 vengono creati e configurati come parte della distribuzione dell'ambiente Amazon EVS. Al momento Amazon EVS supporta solo un singolo gateway Tier-0. Qualsiasi modifica a questi router logici o al nodo perimetrale NSX VMs potrebbe influire sulla connettività e dovrebbe essere evitata.

VMware aggiornamenti software

> **Warning**
>
> Se hai aggiornato la tua versione ESX dopo l'implementazione dell'ambiente Amazon EVS, SDDC Manager potrebbe fallire durante la convalida dell'host VCF nella fase di commissione degli host. Per istruzioni su come risolvere questo problema, consulta. the section called "SDDC Manager non riesce a convalidare l'host VCF durante la messa in servizio dell'host"

Per informazioni sulle versioni VCF fornite da Amazon EVS, consulta. the section called "Versioni VCF e istanze EC2" AWS In base al modello di responsabilità condivisa, l'utente è responsabile dell'applicazione di eventuali patch, aggiornamenti o upgrade al software VCF, tra cui ESX, vCenter Server, vSAN, NSX, SDDC Manager e altre soluzioni integrate, nel proprio ambiente EVS. Dopo la distribuzione, ti consigliamo di esaminare la versione del software VCF distribuita da Amazon EVS e

di aggiornarla secondo necessità. Puoi ottenere gli aggiornamenti VCF tramite il portale di supporto Broadcom. Si consiglia inoltre di stabilire e rispettare un programma di manutenzione regolare per aggiornamenti e patch.

> **Note**
>
> Amazon EVS non supporta VMware Cloud Foundation 9 al momento.

> **Note**
>
> Amazon EVS non fornisce tutte le versioni di VCF ed ESX rilasciate da Broadcom. Per informazioni sull'interoperabilità del software, consulta la Broadcom Interoperability Matrix. Per la piena compatibilità hardware con le istanze AWS EC2, consulta la Broadcom Compatibility Guide.

Alcune patch, aggiornamenti o upgrade possono avere un impatto sui carichi di lavoro in esecuzione nell'ambiente. Prima di applicare patch, aggiornare o aggiornare il software VCF, si consiglia di consultare la VCF Lifecycle Management Guide per comprendere l'impatto di queste modifiche sull'ambiente. Si consiglia inoltre di testare le modifiche in un ambiente di staging prima di implementarle in produzione. È possibile consultare le note di rilascio di VCF 5.2.x per comprendere gli ultimi aggiornamenti di VCF 5.2.x.

Ciclo di vita e manutenzione dell'host ESX

Sei responsabile della gestione e della manutenzione del ciclo di vita degli host ESX all'interno dell'ambiente Amazon EVS, incluso il monitoraggio dello stato dell'host e la risoluzione dei problemi dell'host. Per ulteriori informazioni, consulta the section called “Manutenzione dell'ambiente”.

AWS esegue la manutenzione programmata sulle istanze metalliche EC2 sottostanti per garantire l'affidabilità, la disponibilità e le prestazioni dell'infrastruttura. Per ulteriori informazioni, consulta the section called “Informazioni sulla manutenzione AWS programmata per le istanze EC2”.

Esecuzione della manutenzione sull'ambiente

Questa sezione descrive come eseguire attività di manutenzione comuni per il tuo ambiente Amazon EVS.

Argomenti

Monitora lo stato e le risorse del tuo ambiente

Puoi monitorare vari aspetti del tuo ambiente Amazon EVS e AWS delle risorse sottostanti utilizzando la console Amazon EVS o. AWS CLI

> **Note**
>
> VMware I componenti di Cloud Foundation (VCF) vengono monitorati in SDDC Manager. Non è possibile monitorare i componenti VCF utilizzando la console Amazon EVS o. AWS CLI Per informazioni sull'utilizzo di SDDC Manager per monitorare i componenti di VMware Cloud Foundation (VCF), consulta Guida introduttiva a SDDC Manager.

Visualizza lo stato e le risorse dell'ambiente

Lo stato dell'ambiente consente di determinare se l'ambiente presenta problemi che richiedono attenzione. Segui questa procedura per verificare lo stato dell'ambiente e visualizzare le risorse sottostanti.

Example

Amazon EVS console

1. Apri la console Amazon EVS.
2. Nel riquadro di navigazione, selezionare Compute environments (Ambienti di calcolo).
3. Scegli l'ID dell'ambiente per aprire la pagina dei dettagli dell'ambiente.
4. In Dettagli, visualizza lo stato dell'ambiente.

Se l'ambiente è integro, lo stato viene visualizzato come Superato. In caso di problemi, lo stato viene visualizzato come Non riuscito. Quando lo stato è Non riuscito, è possibile visualizzare un popover che mostra i risultati di quattro controlli dello stato dell'ambiente:

- Riutilizzo della chiave: mostra Passato o Non riuscito per indicare se la chiave di licenza VCF è valida.
- Numero host: mostra Sconosciuto, Passato o Non riuscito per indicare lo stato della connettività dell'host.
- Copertura delle chiavi: mostra Passato o Non riuscito per indicare se la chiave di licenza VCF copre tutti gli host.
- Raggiungibilità: mostra Passato o Non riuscito per indicare la raggiungibilità a SDDC Manager.

  Per informazioni sulla risoluzione dei problemi relativi al controllo dello stato dell'ambiente, vedere. Risoluzione dei problemi

  Per visualizzare le risorse presenti nell'ambiente

  Scegli una delle seguenti schede:

- Host: mostra gli host presenti nell'ambiente.
- Reti e connettività: mostra le risorse VPC, le sottoreti EVS e il VPC Route Server associate al tuo ambiente.
- Dispositivi di gestione: mostra i dispositivi di gestione VCF presenti nell'ambiente con i relativi nomi host DNS e le relative credenziali.
- Tag: mostra i tag associati all'ambiente.

AWS CLI

È possibile utilizzare il AWS CLI per verificare lo stato e le risorse dell'ambiente.

Per elencare tutti gli ambienti e il relativo stato

```
aws evs list-environments
```

> **Tip**
>
> Utilizzate il `--query` parametro per filtrare l'output. Esempio:

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

Per elencare gli host dell'ambiente

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

Per elencare l'ambiente VLANs

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

Per ulteriori informazioni sulle operazioni delle API, consulta quanto segue nella Amazon EVS API Reference Guide:

- ListEnvironments
- ListEnvironmentHosts
- ListEnvironmentVlans

Manutenzione AMI

Amazon EVS distribuisce host ESX con un'Amazon Machine Image (AMI) EVS personalizzata. L'AMI contiene un componente aggiuntivo personalizzato del fornitore contenente i pacchetti necessari per eseguire ESX su Amazon. EC2

Risolvi l'errore di aggiunta dell'host dovuto a un'immagine del cluster incompatibile

Quando aggiungi un host al tuo ambiente, l'host dispone dell'ultima versione disponibile del componente aggiuntivo personalizzato EVS. Se il tuo ambiente utilizza host con una versione del componente aggiuntivo precedente, l'aggiunta di nuovi host non riesce e viene visualizzato un errore che indica che il nuovo host non è compatibile con l'immagine del cluster. Per i passaggi dettagliati

per risolvere questo problema, consultathe section called "Errore di aggiunta dell'host dovuto a un'immagine del cluster incompatibile".

Manutenzione dell'host Amazon EVS

Poiché Amazon EVS è un servizio autogestito, sei responsabile della manutenzione del software VMware Cloud Foundation (VCF) in esecuzione sull'host, del monitoraggio dello stato dell'host e della risoluzione dei problemi dell'host, inclusa la sostituzione dell'host in caso di guasto dell'host. Per ulteriori informazioni sulla gestione degli host ESX in VMware Cloud Foundation (VCF), consulta Host Management nella documentazione di Cloud Foundation. VMware

Verifica dello stato dell'istanza EC2 sottostante

Amazon EC2 esegue i controlli automatici su ogni istanza EC2 in esecuzione per individuare i problemi di hardware e software. Puoi visualizzare i risultati di questi controlli di stato nella console EC2 o AWS CLI identificare problemi specifici e rilevabili. Per ulteriori informazioni, consulta Visualizza i controlli di stato per le istanze Amazon EC2 nella Amazon EC2 User Guide describe-instance-statuse nel AWS CLI Command Line Reference.

Puoi creare un CloudWatch allarme per avvisarti se i controlli di stato falliscono su un'istanza specifica. Per ulteriori informazioni, consulta Crea CloudWatch allarmi per le istanze Amazon EC2 che non superano i controlli di stato nella Guida per l'utente di Amazon EC2.

Informazioni sulla manutenzione AWS programmata per le istanze EC2

AWS esegue la manutenzione programmata sulle istanze EC2 sottostanti per garantire affidabilità, disponibilità e prestazioni. Le istanze bare metal EC2 sono soggette agli stessi tipi di eventi pianificati delle altre istanze EC2. AWS può pianificare eventi per riavviare, arrestare e ritirare le istanze a causa di problemi hardware sottostanti o di manutenzione programmata. Questi eventi non si verificano di frequente. Per ulteriori informazioni, consulta Tipi di eventi programmati nella Guida per l'utente di Amazon EC2.

> **Note**
>
> È necessario mettere gli host in modalità di manutenzione nel vSphere Client prima di qualsiasi evento di riavvio pianificato.

Se una delle tue istanze sarà interessata da un evento programmato, ti AWS avviserà in anticipo via e-mail, utilizzando l'indirizzo email associato al tuo. Account AWS AWS invia anche un evento AWS

Health, che puoi monitorare e gestire utilizzando Amazon EventBridge. Per ulteriori informazioni, consulta Monitoring events in AWS Health with Amazon EventBridge e Scheduled events for Amazon EC2 Instances nella Amazon EC2 User Guide.

In qualsiasi momento, puoi riprogrammare l'evento in modo che si verifichi alla data e all'ora specifiche che preferisci. L'evento può essere ripianificato fino alla data di scadenza dell'evento medesimo. Per ulteriori informazioni, consulta Riprogrammare un evento pianificato per un'istanza EC2 nella Amazon EC2 User Guide.

Utilizzo delle prenotazioni di capacità su richiesta di EC2

Puoi utilizzare le prenotazioni di capacità su richiesta di EC2 per garantire che il cluster disponga di una capacità sufficiente durante i periodi di manutenzione. Puoi riservare la capacità in zone di disponibilità specifiche per qualsiasi durata. Per ulteriori informazioni, consulta Riservare la capacità di calcolo con le prenotazioni di capacità su richiesta EC2 nella Guida per l'utente di Amazon EC2.

Per i passaggi per creare una prenotazione di capacità, consulta Creare una prenotazione di capacità nella Guida per l'utente di Amazon EC2.

> **Note**
>
> Se utilizzi EC2 On-Demand Capacity Reservations o EC2 Dedicated Hosts, ti consigliamo di utilizzare un host di riserva per carichi di lavoro mission critical. Sebbene le prenotazioni di capacità garantiscano l'accesso a una quantità specifica di capacità delle istanze EC2 in una determinata zona di disponibilità, disporre di un host di riserva offre un ulteriore livello di ridondanza, fondamentale per i carichi di lavoro mission critical. Per gli host dedicati, disporre di un host di riserva garantisce la manutenzione dell'ambiente per i carichi di lavoro mission critical, anche se un host primario richiede manutenzione o presenta un problema.

Preparazione del programma e degli eventi AWS `system-maintenance` `instance-retirement`

AWS pianifica due tipi di `system-maintenance` eventi: manutenzione della rete e manutenzione dell'alimentazione.

- Durante la manutenzione della rete, le istanze per le quali è pianificato l'evento perdono la connettività di rete per un breve periodo di tempo. La normale connettività di rete dell'istanza viene ripristinata al completamento della manutenzione.

- Durante la manutenzione dell'alimentazione elettrica, le istanze per le quali è pianificato l'evento vengono impostate sulla modalità offline per un breve periodo di tempo, quindi vengono riavviate. Quando viene eseguito un riavvio su istanze bare metal di EC2, i dati del volume dell'Instance Store non vengono conservati.

AWS pianifica gli `instance-retirement` eventi EC2 quando viene rilevato un degrado dell'hardware sottostante che ospita le istanze EC2.

Per correggere eventuali `system-maintenance` `instance-retirement` eventi, sostituisci l'host guasto con un nuovo host utilizzando la console Amazon EVS o AWS CLI SDDC Manager prima che si verifichi l'evento di manutenzione. Se attendi che si verifichi l'evento di manutenzione ed è necessario il riavvio dell'istanza EC2, perderai i dati vSAN archiviati nel volume dell'instance store. Per informazioni dettagliate sulle fasi, consulta the section called “Sostituisci un host Amazon EVS”.

> **Important**
>
> La console EC2 non deve essere utilizzata per gestire lo stato degli host Amazon EVS, inclusi arresto, avvio e terminazione. Non tentare di avviare, arrestare o terminare le istanze EC2 distribuite da Amazon EVS. Questa azione comporta la perdita di dati vSAN.

Sostituisci un host Amazon EVS

Segui questa procedura per sostituire un host Amazon EVS.

> **Warning**
>
> Gli host Amazon EVS utilizzano un componente aggiuntivo personalizzato del fornitore per fornire importanti funzionalità host. Quando aggiungi un host al tuo ambiente, avrà l'ultima versione disponibile del componente aggiuntivo personalizzato Amazon EVS. Se l'ambiente utilizza host con una versione aggiuntiva precedente, l'aggiunta di host al cluster vSphere causerà un errore nella correzione dell'immagine del cluster. Per le procedure per risolvere questo problema, consulta. the section called “Risolvi l'errore di aggiunta dell'host dovuto a un'immagine del cluster incompatibile”

Warning

Se la versione di ESX è stata aggiornata dopo l'implementazione, SDDC Manager potrebbe fallire durante la convalida dell'host VCF nella fase di commissione degli host. Per la procedura da seguire per risolvere questo problema, consulta. the section called "SDDC Manager non riesce a convalidare l'host VCF durante la messa in servizio dell'host"

Note

Assicurati che il numero di host Amazon EVS per quota di ambiente EVS sia impostato correttamente per garantire la corretta creazione dell'host. La creazione dell'host non riesce se questo valore di quota è inferiore al numero di host che stai tentando di fornire all'interno di un singolo ambiente Amazon EVS. Potrebbe essere necessario richiedere un aumento della quota per le operazioni di manutenzione che richiedono la sostituzione dell'host. Per ulteriori informazioni, consulta Service Quotas.

Example

Amazon EVS console and SDDC Managuer UI

1. Vai alla console Amazon EVS.
2. Nel pannello di navigazione, scegli Ambiente.
3. Seleziona l'ambiente che contiene l'host da sostituire.
4. Seleziona la scheda Host.
5. Scegli Create host (Crea host).
6. Specificate i dettagli dell'host e scegliete Crea host.
7. Per verificare il completamento, verifica che lo stato dell'host sia cambiato in Creato.
8. Recupera le credenziali per la password root di ESX da Secrets Manager AWS . Per ulteriori informazioni sul recupero dei segreti, consulta Ottieni AWS segreti da Secrets Manager nella Guida per l'utente di AWS Secrets Manager.
9. Vai a SDDC Manager.
10. Commissiona il nuovo host in SDDC Manager, utilizzando le credenziali root ESX recuperate nel passaggio precedente. Per ulteriori informazioni, consulta Commission Hosts nella documentazione di Cloud Foundation VMware .

11. Aggiungi il nuovo host al cluster. Per ulteriori informazioni, vedere Come aggiungere un host ESX al cluster vSphere utilizzando il flusso di lavoro Quickstart nella documentazione di vSphere.
12. Rimuovi il vecchio host in SDDC Manager che desideri rimuovere da SDDC Manager. Per ulteriori informazioni, consulta la documentazione Decommission Hosts nella documentazione di Cloud Foundation VMware .
13. Torna alla console Amazon EVS.
14. Nella scheda Host, seleziona l'host guasto e scegli Elimina > Elimina host.

AWS CLI and SDDC Manager UI

1. Apri una nuova sessione terminale.
2. Crea un nuovo host. Vedi il comando di esempio riportato di seguito per riferimento.

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

3. Recupera le credenziali per la password root di ESX da Secrets Manager AWS . Per ulteriori informazioni sul recupero dei segreti, consulta Ottieni AWS segreti da Secrets Manager nella Guida per l'utente di AWS Secrets Manager.
4. Vai a SDDC Manager.
5. Commissiona il nuovo host in SDDC Manager, utilizzando le credenziali root ESX recuperate nel passaggio precedente. Per ulteriori informazioni, consulta Commission Hosts nella documentazione di Cloud Foundation VMware .
6. Aggiungi il nuovo host al cluster che contiene l'host danneggiato.
7. Disattiva l'host danneggiato in SDDC Manager. Per ulteriori informazioni, consulta la documentazione Decommission Hosts nella documentazione di Cloud Foundation VMware .
8. Ritorna al terminale.
9. Eliminare l'host fallito. Per riferimento, vedi il comando di esempio riportato di seguito.

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

Risoluzione dei problemi

Linee guida Broadcom and AWS Support

AWS fornisce supporto per Amazon EVS e i servizi di infrastruttura associati, tra cui VMware Cloud Foundation (VCF). Per indicazioni sulla configurazione specifiche di VCF o problemi relativi ad altri VMware prodotti come Aria Suite, HCX o NSX, puoi anche contattare Broadcom direttamente utilizzando i tuoi diritti di supporto Broadcom. Per ulteriori informazioni, consulta Broadcom Support Portal.

Per una guida alla risoluzione dei problemi, consultaRisoluzione dei problemi. Se continui a riscontrare problemi dopo aver consultato la guida alla risoluzione dei problemi, contatta AWS il Supporto per ulteriore assistenza.

Configura una tabella di routing personalizzata per le sottoreti Amazon EVS

Amazon EVS supporta l'uso di una tabella di routing personalizzata solo dopo la creazione dell'ambiente Amazon EVS. Per consentire una corretta creazione dell'ambiente, è necessario configurare la tabella di routing principale per consentire il traffico verso servizi dipendenti come DNS e sistemi locali. Questo perché le sottoreti VLAN di Amazon EVS sono associate implicitamente alla tabella di routing principale del nostro VPC durante la distribuzione dell'ambiente.

Dopo la distribuzione dell'ambiente, devi associare esplicitamente ciascuna delle sottoreti VLAN di Amazon EVS a una tabella di routing nel tuo VPC. La connettività NSX fallisce se le sottoreti VLAN non sono associate esplicitamente a una tabella di routing VPC. Ti consigliamo vivamente di associare esplicitamente le tue sottoreti a una tabella di routing personalizzata. Una tabella di routing personalizzata offre un controllo più granulare sul routing del traffico di rete all'interno del VPC, consentendo regole di routing personalizzate per sottoreti o gateway specifici. Per ulteriori informazioni sulla creazione di una tabella di routing personalizzata, consulta Create a route table for your VPC nella Amazon VPC User Guide.

Configura una lista di controllo degli accessi alla rete per controllare il traffico della sottorete VLAN di Amazon EVS

Una lista di controllo degli accessi (ACL) di rete consente o nega traffico specifico in entrata o in uscita a livello di sottorete. Puoi utilizzare la rete ACLs per controllare il traffico in entrata e in uscita per le sottoreti VLAN di Amazon EVS. Per ulteriori informazioni, consulta Creare un ACL di rete per il tuo VPC nella Amazon VPC User Guide.

Important

EC2 i gruppi di sicurezza non funzionano su interfacce di rete elastiche collegate alle sottoreti VLAN di Amazon EVS. Per controllare il traffico da e verso le sottoreti VLAN di Amazon EVS, devi utilizzare una lista di controllo degli accessi alla rete.

Warning

Amazon EVS richiede l'accesso alla tua distribuzione VCF. È necessario configurare i gruppi di sicurezza e le liste di controllo degli accessi alla rete (ACLs) per consentire ad Amazon EVS di comunicare con:

- Server DNS sulla TCP/UDP porta 53.
- Sottorete VLAN di gestione dell'host tramite HTTPS e SSH.
- Sottorete VLAN VM di gestione tramite HTTPS e SSH.

Se i gruppi di sicurezza e la rete ACLs non consentono questo accesso, l'implementazione dell'ambiente Amazon EVS fallirà e gli ambienti esistenti potrebbero presentare uno stato di conformità degradato.

Ciclo di vita della gestione segreta

Amazon EVS utilizza AWS Secrets Manager per creare, crittografare e archiviare segreti nel tuo account durante la distribuzione iniziale dell'ambiente. Questi segreti contengono le credenziali VCF necessarie per installare e accedere ai dispositivi di gestione VCF come vCenter Server, NSX e SDDC Manager, nonché la password root dell'host ESX. Amazon EVS elimina anche i segreti gestiti per tuo conto quando l'ambiente EVS viene eliminato.

Sei responsabile della gestione segreta del ciclo di vita, inclusa la rotazione segreta. Amazon EVS non fornisce una rotazione gestita dei segreti. Ti consigliamo di ruotare i segreti regolarmente su una finestra di rotazione prestabilita per assicurarti che i segreti non durino a lungo. Per ulteriori informazioni, consulta Pianificazioni di rotazione nella Guida per l'utente di AWS Secrets Manager.

Crea un host Amazon EVS

Dopo l'implementazione di un ambiente Amazon EVS, puoi aggiungere host per aumentare la capacità e la resilienza del carico di lavoro. Amazon EVS supporta 4-32 host e una larghezza di banda di throughput predefinita fino a 600 Gbps per ambiente. Questa azione può essere utilizzata solo dopo la distribuzione dell'ambiente Amazon EVS.

> **Note**
>
> È necessario assegnare e mettere in servizio l'host all'interno dell'interfaccia utente di SDDC Manager.

Per creare un host Amazon EVS

Segui questi passaggi per creare un host Amazon EVS.

> **Warning**
>
> Gli host Amazon EVS utilizzano l'Amazon EVS Custom Addon per fornire importanti funzionalità host. Quando aggiungi un host al tuo ambiente, avrà l'ultima versione disponibile di Amazon EVS Custom Addon. Se l'ambiente utilizza host con una versione precedente di Custom Addon, l'aggiunta di host al cluster vSphere causerà un errore nella correzione dell'immagine del cluster. Per la procedura da seguire per risolvere questo problema, consulta. the section called “Risolvi l'errore di aggiunta dell'host dovuto a un'immagine del cluster incompatibile”

> **Warning**
>
> Se hai aggiornato la tua versione ESX dopo l'implementazione dell'ambiente Amazon EVS, SDDC Manager potrebbe fallire durante la convalida dell'host VCF nella fase di commissione

degli host. Per istruzioni su come risolvere questo problema, consulta. the section called "SDDC Manager non riesce a convalidare l'host VCF durante la messa in servizio dell'host"

> **Note**
>
> Assicurati che il numero di host Amazon EVS per quota di ambiente EVS sia impostato correttamente per garantire la corretta creazione dell'host. La creazione dell'host non riesce se questo valore di quota è inferiore al numero di host che stai tentando di fornire all'interno di un singolo ambiente Amazon EVS. Per aumentare la quota, puoi richiedere un aumento della quota. Per ulteriori informazioni, consulta Service Quotas.

> **Note**
>
> Se non specifichi una versione ESX quando aggiungi host al tuo ambiente, Amazon EVS utilizza automaticamente la versione ESX predefinita associata alla versione VCF del tuo ambiente. Per ulteriori informazioni, consulta the section called "Versioni VCF e istanze EC2".

> **Important**
>
> Quando si aggiunge un host ESX, selezionare una versione ESX che corrisponda al cluster vSphere di destinazione. Se la stessa versione non è disponibile, implementa una versione precedente ed esegui l'upgrade utilizzando vSphere Lifecycle Manager. Per ulteriori informazioni, consulta the section called "SDDC Manager non riesce a convalidare l'host VCF durante la messa in servizio dell'host". Gli upgrade possono richiedere il riavvio dell'host e aumentare il tempo necessario per la messa in servizio dell'host.
> Un host con una versione ESX più recente della versione ESX dell'immagine del cluster vSphere non può essere sottoposto a downgrade. Sarà necessario eliminare l'host e ricrearlo con la versione ESX corretta.

Example

Amazon EVS console and SDDC Managuer UI

1. Vai alla console Amazon EVS.

2. Nel pannello di navigazione, scegli Ambiente.
3. Seleziona l'ambiente in cui desideri creare l'host.
4. Seleziona la scheda Host.
5. Scegli Create host (Crea host).
6. Specificate i dettagli dell'host e scegliete Crea host.
7. Per verificare il completamento, verifica che lo stato dell'host sia cambiato in Creato.
8. Vai a SDDC Manager.
9. Commissiona il nuovo host in SDDC Manager. Per ulteriori informazioni, consulta Commission Hosts nella documentazione di VMware Cloud Foundation.
10. Aggiungi il nuovo host al cluster utilizzando SDDC Manager. Per ulteriori informazioni, vedere Come aggiungere un host ESX al cluster vSphere utilizzando il flusso di lavoro Quickstart nella documentazione di vSphere.

AWS CLI and SDDC Manager UI

1. Aprire una nuova sessione di terminale.
2. Crea un nuovo host. Vedi il comando di esempio riportato di seguito per riferimento.

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

3. Vai a SDDC Manager.
4. Commissiona il nuovo host in SDDC Manager. Per ulteriori informazioni, consulta Commission Hosts nella documentazione di VMware Cloud Foundation.
5. Aggiungi il nuovo host al cluster utilizzando SDDC Manager. Per ulteriori informazioni, vedere Come aggiungere un host ESX al cluster vSphere utilizzando il flusso di lavoro Quickstart nella documentazione di vSphere.

Eliminare un host Amazon EVS

Puoi eliminare un host Amazon EVS dal tuo ambiente quando l'host non è più necessario. Amazon EVS richiede che il tuo ambiente abbia un minimo di quattro host. Amazon EVS non supporta ambienti con meno di quattro host.

> **Warning**
>
> L'eliminazione di un host senza disattivazione lascerà dati obsoleti in vCenter e SDDC Manager, il che potrebbe richiedere ulteriori interventi di pulizia. Assicurati che i tuoi host siano disattivati prima di eliminare gli host nella console o nell'API di Amazon EVS.

> **Warning**
>
> Usa sempre la console o l'API Amazon EVS per rimuovere i tuoi host Amazon EVS. L'eliminazione degli host dalla EC2 console può lasciare l'ambiente in uno stato incoerente.

Per eliminare un host Amazon EVS

Segui questi passaggi per eliminare un host Amazon EVS.

Example

SDDC Managuer UI and Amazon EVS console

1. Vai a SDDC Manager.
2. Rimuovi il cluster da SDDC Manager.
3. Disattiva l'host in SDDC Manager. Per ulteriori informazioni, consulta la documentazione Decommission Hosts nella documentazione di VMware Cloud Foundation.
4. Vai alla console Amazon EVS.
5. Nel pannello di navigazione, scegli Ambiente.
6. Seleziona l'ambiente che contiene l'host da eliminare.
7. Seleziona la scheda Host.
8. Scegli Elimina host.

9. Seleziona l'host e scegli Elimina nella scheda Host. Ripeti questo passaggio per ogni host che desideri eliminare.

SDDC Manager UI and AWS CLI

1. Vai a SDDC Manager.
2. Rimuovi il cluster da SDDC Manager.
3. Disattiva l'host in SDDC Manager. Per ulteriori informazioni, consulta la documentazione Decommission Hosts nella documentazione di VMware Cloud Foundation.
4. Apri una nuova sessione di terminale.
5. Eliminare l'host. Per riferimento, vedi il comando di esempio riportato di seguito.

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

Crea un connettore per l'ambiente Amazon EVS

Puoi creare un connettore per consentire ad Amazon EVS di comunicare con un'appliance di gestione VCF, come vCenter Server, nel tuo ambiente. Un connettore utilizza il nome di dominio completo (FQDN) per l'appliance e le credenziali archiviate in un segreto di Secrets Manager AWS per l'autenticazione con l'appliance.

Ulteriori informazioni sui connettori sono disponibili in Concetti e componenti di Amazon EVS.

Warning

Prima di creare un connettore, si consiglia di creare un utente vCenter dedicato con un ReadOnly ruolo. Evita di utilizzare credenziali con autorizzazioni elevate o amministrative.

Note

Prima di creare un connettore, è necessario creare un segreto in AWS Secrets Manager con le credenziali dell'appliance. Il segreto deve contenere due chiavi `username` e. `password`

I valori devono essere le credenziali di accesso per l'utente dedicato creato per l'appliance specificata nel connettore.

Important

È necessario aggiungere il tag `EvsAccess=true` al segreto di Secrets Manager. Se hai crittografato il segreto con il tuo AWS KMS key, aggiungi il `EvsAccess=true` tag AWS KMS key anche a.

Note

Ogni connettore è mappato a un singolo FQDN dell'appliance.

Note

È consentito un solo connettore di tipo vCenter per ambiente.

Note

L'FQDN deve essere valido, corrispondere al nome di dominio utilizzato durante la creazione dell'ambiente EVS ed essere univoco per tutti i connettori dell'ambiente.

Note

La creazione del connettore non convalida la raggiungibilità o le credenziali dell'appliance. Dopo che lo stato del connettore è Attivo, lo stato del controllo di raggiungibilità verrà aggiornato da Sconosciuto a Passato o Fallito in modo asincrono entro 10 minuti.

Per creare un connettore di ambiente Amazon EVS

Segui questi passaggi per creare un connettore Amazon EVS.

Example

Amazon EVS console

1. Vai alla console Amazon EVS.
2. Nel riquadro di navigazione, selezionare Compute environments (Ambienti di calcolo).
3. Seleziona l'ambiente in cui desideri creare il connettore.
4. Seleziona la scheda Connettori.
5. Scegli Create connector (Crea connettore).
6. Per Appliance FQDN, inserire il nome di dominio completo dell'appliance.
7. Per il menu a discesa Secrets Manager, selezionare il Segreto contenente le credenziali dell'appliance.
8. Scegli Create connector (Crea connettore).
9. Per verificare il completamento, verifica che lo stato del connettore sia Attivo e che il risultato del controllo di raggiungibilità sia Passato.

AWS CLI

1. Apri una nuova sessione di terminale.
2. Crea un nuovo connettore. Per riferimento, vedi il comando di esempio riportato di seguito.
   - l'identificatore segreto può essere il nome segreto o l'ARN

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

3. Per verificare il completamento, utilizzate il list-environment-connectorscomando e verificate che lo stato del connettore sia Attivo e che il risultato del controllo di raggiungibilità sia passato.

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

Aggiornamento di un connettore di ambiente Amazon EVS

È possibile aggiornare un connettore esistente per modificare il nome di dominio completo dell'appliance o puntare a un altro segreto di Secrets Manager per l'autenticazione. Ad esempio, potrebbe essere necessario aggiornare l'FQDN se l'endpoint dell'appliance cambia o passare a un segreto diverso. È inoltre possibile aggiornare i valori del segreto esistente di Secrets Manager direttamente durante la rotazione delle credenziali vCenter, in modo che non sia richiesto alcun aggiornamento del connettore.

Ulteriori informazioni sui connettori sono disponibili in Concetti e componenti di Amazon EVS.

> **Note**
>
> È possibile aggiornare solo una proprietà di un connettore alla volta.

> **Note**
>
> Il connettore deve trovarsi nello stato Attivo o Aggiornamento non riuscito per poter essere aggiornato.

> **Note**
>
> Se si aggiorna l'FQDN, il nuovo FQDN deve essere valido, corrispondere al nome di dominio utilizzato durante la creazione dell'ambiente EVS ed essere univoco per tutti i connettori dell'ambiente.

Per aggiornare un connettore di ambiente Amazon EVS

Segui questi passaggi per aggiornare un connettore Amazon EVS.

Example

Amazon EVS console

1. Vai alla console Amazon EVS.

2. Nel riquadro di navigazione, selezionare Compute environments (Ambienti di calcolo).
3. Seleziona l'ambiente contenente il connettore.
4. Seleziona la scheda Connettori.
5. Seleziona il connettore che desideri aggiornare.
6. Scegli Azioni, quindi nel menu a discesa seleziona Update Secret o Aggiorna FQDN.
7. Per Update Secret:
   a. Nel menu a discesa segreto, seleziona il segreto con le credenziali dell'appliance e scegli Aggiorna.
8. Per Update FQDN:
   a. Inserisci il nuovo FQDN e scegli Aggiorna.
9. Per verificare il completamento, verifica che lo stato del connettore sia tornato ad Attivo dall'aggiornamento.

AWS CLI

1. Apri una nuova sessione di terminale.
2. Aggiorna il segreto o l'FQDN del connettore. Per riferimento, vedi i comandi di esempio riportati di seguito.

   Per aggiornare il segreto:

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

   Per aggiornare il nome di dominio completo:

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

3. Per verificare il completamento, usa il list-environment-connectorscomando e verifica che lo stato del connettore sia Attivo.

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

Eliminare un connettore di ambiente Amazon EVS

È possibile eliminare un connettore quando non è più necessario.

Ulteriori informazioni sui connettori sono disponibili in Concetti e componenti di Amazon EVS.

> **Note**
>
> Il connettore deve essere in uno stato Attivo, Create Failed o Update Failed per essere eliminato.

> **Note**
>
> Tutti i permessi associati al connettore devono essere eliminati prima che il connettore possa essere rimosso.

Per eliminare un connettore di ambiente Amazon EVS

Segui questi passaggi per eliminare un connettore Amazon EVS.

Example

Amazon EVS console

1. Vai alla console Amazon EVS.
2. Nel riquadro di navigazione, selezionare Compute environments (Ambienti di calcolo).
3. Seleziona l'ambiente contenente il connettore.
4. Seleziona la scheda Connettori.
5. Seleziona il connettore che desideri eliminare.
6. Scegli Elimina connettore.

7. Conferma l'eliminazione.
8. Per verificare il completamento, verifica che il connettore non compaia più nell'elenco.

AWS CLI

1. Aprire una nuova sessione di terminale.
2. Eliminare il connettore. Per riferimento, vedi il comando di esempio riportato di seguito.

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

3. Per verificare il completamento, usa il list-environment-connectorscomando e conferma che il connettore non è più nell'elenco.

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

Crea un'autorizzazione Amazon EVS

Puoi creare diritti Windows Server per una o più macchine virtuali (VMs) in esecuzione nel tuo ambiente Amazon EVS. Dopo aver creato un'autorizzazione e aver acceso la macchina virtuale, Amazon EVS inizia a monitorare l'utilizzo delle autorizzazioni Windows Server della macchina virtuale corrispondente, consentendoti di utilizzare le licenze di Windows Server direttamente su base regolare. AWS pay-as-you-go

Ulteriori informazioni sui diritti sono disponibili in Concetti e componenti di Amazon EVS.

> **Note**
>
> È possibile creare solo 100 diritti alla volta.

> **Note**
>
> È necessario creare un connettore vCenter prima di creare i permessi. Il connettore deve essere in uno stato Attivo e il correttore di raggiungibilità deve essere in uno stato Passato.

> **Note**
>
> La convalida avviene in modo asincrono. Se una macchina virtuale non riesce a convalidare (ad esempio, sistema operativo guest non supportato o macchina virtuale non trovata), lo stato di autorizzazione viene impostato su Creazione non riuscita con dettagli di errore. È possibile risolvere il problema sottostante, quindi creare nuovamente l'autorizzazione.

> **Note**
>
> In vCenter è possibile utilizzare PowerCLI o altri strumenti per ottenere il VM Managed Object ID.

Per creare un'autorizzazione Amazon EVS

Segui questi passaggi per creare un'autorizzazione Amazon EVS.

Example

Amazon EVS console

1. Vai alla console Amazon EVS.
2. Nel riquadro di navigazione, selezionare Compute environments (Ambienti di calcolo).
3. Seleziona l'ambiente contenente il. VMs
4. Seleziona la scheda Entitlements.
5. Scegliere Aggiungi.
6. Per impostazione predefinita, il tipo di prodotto è Windows Server.
7. Aggiungi i diritti per VMs cui desideri creare i permessi tramite testo o caricando un file CSV.
   - Il formato CSV è una singola colonna della sola VM. IDs
8. Scegli Aggiungi autorizzazione.
9. Per verificare il completamento, verifica che lo stato dell'autorizzazione sia cambiato in Creato.

AWS CLI

1. Apri una nuova sessione di terminale.

2. Crea diritti. Per riferimento, vedi il comando di esempio riportato di seguito.

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

3. Per verificare il completamento, elenca le autorizzazioni della macchina virtuale e verifica che lo stato delle autorizzazioni sia Creato.

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

Eliminare un'autorizzazione Amazon EVS

Puoi eliminare le autorizzazioni di Windows Server per una o più macchine virtuali (VMs) nel tuo ambiente Amazon EVS. Quando elimini un'autorizzazione, Amazon EVS interrompe il monitoraggio dell'utilizzo delle autorizzazioni di Windows Server per la macchina virtuale specificata. Dopo l'eliminazione, la macchina virtuale non dispone più dell'autorizzazione a Windows Server. AWS

Ulteriori informazioni sui diritti sono disponibili in Concetti e componenti di Amazon EVS.

> **Note**
>
> Puoi eliminare solo fino a 100 diritti alla volta.

> **Note**
>
> È necessario specificare la macchina virtuale da cui IDs eliminare i permessi.

> **Note**
>
> Dopo l'eliminazione, non VMs saranno più disponibili i permessi di Windows Server. AWS

Per eliminare un'autorizzazione Amazon EVS

Segui questi passaggi per eliminare un'autorizzazione Amazon EVS.

Example

Amazon EVS console

1. Vai alla console Amazon EVS.
2. Nel riquadro di navigazione, selezionare Compute environments (Ambienti di calcolo).
3. Seleziona l'ambiente contenente il. VMs
4. Seleziona la scheda Entitlements.
5. Seleziona la cartella VMs da cui desideri eliminare i diritti.
6. Scegli Elimina.
7. Conferma la rimozione.
8. Per verificare il completamento, verifica che i diritti relativi alla specifica operazione siano VMs stati rimossi dall'elenco delle console.

AWS CLI

1. Apri una nuova sessione di terminale.
2. Eliminare un diritto. Per riferimento, vedi il comando di esempio riportato di seguito.

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

3. Per verificare il completamento, elenca i diritti e conferma che VMs quelli eliminati non sono più presenti.

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

Configurazione dell'attivazione di Windows Server

Amazon EVS fornisce l'attivazione di Windows Server per macchine virtuali con diritti Windows Server. È necessario creare un endpoint VPC per l'attivazione di EVS Windows Server all'interno del VPC utilizzato per l'ambiente Amazon EVS. Ogni macchina virtuale autorizzata deve quindi essere configurata per connettersi a questo endpoint di attivazione. Gli endpoint VPC possono essere creati solo se disponi di un ambiente Amazon EVS attivo.

1. Identifica il VPC in cui viene distribuito l'ambiente Amazon EVS.
2. Nello stesso VPC, crea un endpoint VPC utilizzando il seguente nome di servizio:

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

   Ad esempio, crea un endpoint VPC con la seguente configurazione:

   - Tipo: servizi AWS
   - Nome del servizio: cerca e seleziona `com.amazonaws.region.evs-windows-server-activation`
   - VPC: seleziona il VPC in cui risiede il tuo ambiente Amazon EVS
   - Sottoreti: seleziona le sottoreti da cui le tue macchine virtuali Windows stabiliscono connessioni in uscita
   - Gruppi di sicurezza: selezionane o creane uno che consenta la porta TCP in entrata 1688 dal gruppo di sicurezza o CIDR dell'istanza Windows
3. Annota il nome DNS privato dell'endpoint VPC che hai creato.
4. Connect alla VM Windows Server e apri PowerShell.
5. Configura il server di attivazione per utilizzare l'endpoint VPC eseguendo il seguente comando:

   ```
   cscript C:\Windows\System32\slmgr.vbs /skms VPC_Endpoint_Private_DNS_Name:1688
   ```

   L'output conferma che il server di attivazione è stato impostato correttamente.
6. Attiva Windows Server eseguendo il comando seguente:

   ```
   cscript C:\Windows\System32\slmgr.vbs /ato
   ```

   L'output deve includere `Product activated successfully.`
7. Verificate che l'attivazione sia stata completata correttamente eseguendo il comando seguente:

```
cscript C:\Windows\System32\slmgr.vbs /dli
```

L'output dovrebbe includere:

- `Volume activation expiration: 259200 minute(s) (180 day(s))`— o vicino ad esso
- `Registered KMS machine name: VPC_Endpoint_Private_DNS_Name:1688`

Risoluzione dei problemi

L'attivazione non riesce perché la VM non dispone di un GVLK

L'endpoint di attivazione EVS richiede che sulle VM sia installata una Generic Volume License Key (GVLK) per utilizzare l'attivazione. KMS-based Per verificare se è installato un GVLK, esegui il seguente comando:

```
cscript C:\Windows\System32\slmgr.vbs /dlv | findstr /C:"Product Key Channel"
```

Se l'output non viene visualizzato`Volume:GVLK`, trova il codice prodotto corrispondente (GVLK) per la tua versione e edizione di Windows dai codici di attivazione del client KMS sul sito Web di Microsoft. Installalo eseguendo il seguente comando:

```
cscript C:\Windows\System32\slmgr.vbs /ipk GVLK
```

Dopo aver installato GVLK, riprova i passaggi di attivazione a partire dal comando nel passaggio 6. `/ato`

Il comando di attivazione restituisce un errore

Se `cscript C:\Windows\System32\slmgr.vbs /ato` restituisce un errore, verifica che la VM possa raggiungere l'endpoint VPC sulla porta 1688:

```
Test-NetConnection -ComputerName VPC_Endpoint_Private_DNS_Name -Port 1688
```

L'output dovrebbe essere visualizzato. `TcpTestSucceeded : True` Esempio:

```
ComputerName     : <VPC_Endpoint_Private_DNS_Name>
```

```
RemoteAddress    : <VPC_Endpoint_IP_address>
RemotePort       : 1688
InterfaceAlias   : Ethernet 2
SourceAddress    : 10.0.110.93
TcpTestSucceeded : True
```

In caso `TcpTestSucceeded` `False` affermativo, verifica che il gruppo di sicurezza VPC Endpoint consenta la porta TCP 1688 in entrata dal gruppo di sicurezza della VM o CIDR.

Accedi al deposito Amazon EVS Custom Addon

Amazon EVS fornisce un depot di addon personalizzato che puoi configurare come sorgente di download in vSphere Lifecycle Manager (vLCM). Utilizza l'azione `GetDepotUrl` API per recuperare un URL e un token di autenticazione per il depot.

> **Note**
>
> Il supporto della console per il depot Custom Addon non è al momento disponibile. Utilizza la AWS CLI o l'API.

Come funziona il deposito Custom Addon

Quando crei un ambiente Amazon EVS, viene fornito automaticamente un token di accesso al deposito. Puoi utilizzare l'azione `GetDepotUrl` API per recuperare un URL che include questo token. Configura questo URL come sorgente di download in vLCM per sincronizzare e installare l'Amazon EVS Custom Addon.

> **Note**
>
> Il token di accesso al depot rimane attivo fino a quando non viene ruotato esplicitamente utilizzando il flag. `--rotate`

Prerequisiti

Prima di poter accedere al depot di Custom Addon, devi disporre di quanto segue:

- Un ambiente Amazon EVS nello `CREATED` stato.

- Autorizzazioni IAM per avviare l'azione`evs:GetDepotUrl`. Per ulteriori informazioni, consulta the section called "Esempi di policy basate sull'identità di Amazon EVS".

Ottenere un URL di depot

Puoi ottenere un URL di deposito utilizzando la AWS CLI.

AWS CLI

Usa il `get-depot-url` comando per recuperare un URL di depot per il tuo ambiente.

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

La risposta include l'URL del depot e il token di autenticazione:

```
{
    "depotUrl": "https://example.cloudfront.net/<token>/depot/vmw-depot-index.xml",
    "token": "<authentication-token>"
}
```

Utilizzo dell'URL del depot

Dopo aver recuperato l'URL del depot, configuralo come sorgente di download in vSphere Lifecycle Manager (vLCM) per sincronizzare e installare l'Amazon EVS Custom Addon.

1. Accedere al vSphere Client.
2. Accedere a vSphere Lifecycle Manager.
3. Aggiungi l'URL del depot come nuova fonte di download.

> **Note**
>
> L'utente vSphere deve disporre del `VMware vSphere Lifecycle Manager > Configure` privilegio.

Per istruzioni dettagliate sull'aggiunta di una fonte di download, consulta Aggiungere una nuova fonte di download nella documentazione di Broadcom.

Rotazione del token di accesso al deposito

Per ruotare il token di accesso al depot, usa il `get-depot-url` comando con la bandiera: `--rotate`

```
aws evs get-depot-url --environment-id env-abcde12345 --rotate
```

Dopo la rotazione, gli URL di deposito precedentemente emessi smetteranno di funzionare entro 5 minuti. È necessario configurare il nuovo URL di depot in vLCM.

autorizzazioni IAM

Per accedere al depot Custom Addon, la tua identità IAM deve essere autorizzata a `evs:GetDepotUrl` intervenire sulle risorse del tuo ambiente. Per ulteriori informazioni, consulta the section called "Esempi di policy basate sull'identità di Amazon EVS".

Sicurezza in Amazon Elastic VMware Service

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS te e te. Il modello di responsabilità condivisa descrive questo come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gira Servizi AWS su Cloud AWS. AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. I revisori di terze parti testano e verificano regolarmente l'efficacia della sicurezza come parte dei programmi di conformitàAWS. Per ulteriori informazioni sui programmi di conformità che si applicano ad Amazon Elastic VMware Service (Amazon EVS), consulta Servizi AWS Scope by Compliance Program.
- Sicurezza nel cloud: la tua responsabilità è determinata dall'uso Servizio AWS che utilizzi. L'utente è anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della propria azienda e le leggi e normative vigenti.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa quando usi Amazon EVS. Ti mostra come configurare Amazon EVS per soddisfare i tuoi obiettivi di sicurezza e conformità. Scopri anche come utilizzarne altri Servizi AWS che ti aiutano a monitorare e proteggere le tue risorse Amazon EVS.

Indice

Protezione dei dati in Amazon EVS

Il modello di responsabilitàAWS condivisa si applica alla protezione dei dati in Amazon Elastic VMware Service. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutto il AWS cloud. L'utente è responsabile del mantenimento del controllo sui contenuti ospitati su questa infrastruttura, inclusi i componenti di VMware Cloud Foundation (VCF). Sei inoltre responsabile delle attività di configurazione e gestione della sicurezza

relative ai file Servizi AWS che utilizzi. Per ulteriori informazioni sulla privacy dei dati, consulta Domande frequenti sulla privacy dei dati. Per ulteriori informazioni sulla protezione dei dati, consulta il post del blog Modello di responsabilità condivisa di AWS e GDPR sul Blog della sicurezza di AWS .

Ai fini della protezione dei dati, ti consigliamo di proteggere Account AWS le credenziali e di configurare i singoli utenti con AWS IAM Identity Center o AWS Identity and Access Management. In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- SSL/TLS Da utilizzare per comunicare con AWS le risorse. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail. Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta Lavorare con i CloudTrail percorsi nella Guida per l' AWS CloudTrail utente.

> **Note**
>
> Amazon EVS non registra le attività degli utenti per elementi non AWS componenti, ad esempio le attività all'interno dell'ambiente VCF. Queste attività vengono registrate in varie VMware console come vSphere e NSX Manager. Se si desidera una registrazione VCF centralizzata, è possibile configurare soluzioni di monitoraggio VCF come VMware Aria Operations o Tanzu Observability per ottenere questo risultato. VMware Per ulteriori informazioni, consulta VMware Cloud Foundation con VMware Tanzu e VMware Aria Suite Lifecyle in modalità Cloud Foundation nella documentazione VCF. VMware

- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno. Servizi AWS
- Utilizza servizi di sicurezza gestiti avanzati come Amazon Macie, che aiutano a scoprire e proteggere i dati sensibili archiviati in. Amazon S3
- Se hai bisogno di moduli crittografici convalidati FIPS 140-3 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-3.

Ti consigliamo vivamente di non inserire mai informazioni identificative sensibili, come gli indirizzi e-mail dei tuoi clienti, nei tag o nei campi di testo in formato libero come il campo Nome. Ciò include quando lavori con Amazon EVS o altro Servizi AWS utilizzando la console, l'API o AWS SDKs. AWS

CLI I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando si fornisce un URL a un server esterno, suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la richiesta al server.

Crittografia dei dati a riposo

Amazon EVS implementa istanze metalliche EC2 che utilizzano la crittografia AES-256 trasparente per impostazione predefinita per i dati archiviati nel volume dell'instance store. Amazon EVS non supporta al momento la crittografia del volume di avvio EBS.

Volume di avvio di Amazon EBS

Le istanze Amazon EVS utilizzano un volume di avvio Amazon EBS. Il volume di avvio contiene il sistema operativo e altri file necessari per l'avvio e l'esecuzione dell'istanza EC2. Il volume di avvio non è crittografato. Al momento Amazon EVS non supporta la crittografia dei volumi di avvio. Il volume di avvio non contiene dati utente provenienti dalle macchine virtuali.

Volume di instance store

Le istanze in metallo Amazon EVS EC2 sono dotate di storage NVMe SSD locale, che fa parte dell'hardware dell'istanza. Amazon EVS utilizza i volumi di NVMe instance store come dischi per i datastore vSAN. Il datastore vSAN contiene le macchine virtuali di gestione e carico di lavoro dopo la distribuzione dell'ambiente Amazon EVS.

I dati sui volumi dell' NVMe Instance Store vengono crittografati utilizzando un codice XTS-AES-256, implementato su un modulo hardware sull'istanza. Le chiavi utilizzate per crittografare i dati scritti su dispositivi di storage collegati localmente sono per cliente e per volume NVMe . Per ulteriori informazioni, consulta Encryption at rest nella Amazon EC2 User Guide.

Dopo aver distribuito l'ambiente Amazon EVS, puoi abilitare la data-at-rest crittografia vSAN per tutti i dati archiviati nel datastore vSAN, per singole macchine virtuali () VMs o per singoli file all'interno. VMs Questo controllo granulare può essere utile quando alcuni VMs richiedono la crittografia mentre altri no, o quando è necessario crittografare dischi o file specifici all'interno di una macchina virtuale. Per ulteriori informazioni, vedere How vSAN Data-At-Rest Encryption Works nella documentazione di vSAN VMware .

Crittografia dei dati in transito

Amazon EVS non crittografa il traffico in transito per impostazione predefinita. Per crittografare i dati in transito che attraversano Amazon EVS, puoi utilizzare la crittografia a livello di applicazione con un protocollo come Transport Layer Security (TLS). Per ulteriori informazioni sulla crittografia del traffico delle istanze EC2, consulta Encryption in Transit nella Amazon EC2 User Guide.

> **Note**
>
> La crittografia di rete Nitro non si applica alle istanze EC2 distribuite da Amazon EVS. Amazon EVS non supporta la crittografia in transito del traffico tra host.

Opzioni di crittografia in transito per la connettività locale

Per crittografare il traffico tra il tuo data center locale e Amazon EVS, puoi combinare l'uso di AWS Direct Connect e AWS Site-To-Site VPN con Transit Gateway AWS . Questa combinazione fornisce una connessione privata IPsec crittografata che riduce anche i costi di rete, aumenta la velocità di trasmissione della larghezza di banda e offre un'esperienza di rete più coerente rispetto alle connessioni VPN basate su Internet. Per ulteriori informazioni, consulta Private IP AWS Site-to-Site VPN con AWS Direct Connect.

> **Note**
>
> Amazon EVS non supporta la connettività tramite un'interfaccia virtuale privata (VIF) AWS Direct Connect o tramite una connessione AWS Site-to-Site VPN che termina direttamente nel VPC sottostante. Amazon EVS supporta la terminazione IPSec VPN sul gateway NSX Edge Tier-0 o Tier-1. Per ulteriori informazioni, consulta Aggiungere un servizio VPN NSX nella documentazione di NSX IPSec . VMware

MAC Security (MACsec) è uno standard IEEE che garantisce la riservatezza dei dati, l'integrità dei dati e l'autenticità dell'origine dei dati. È possibile utilizzare connessioni AWS Direct Connect che supportano MACsec la crittografia dei dati dal data center aziendale alla posizione AWS Direct Connect. Per ulteriori informazioni, consulta la sezione Sicurezza MAC in AWS Direct Connect nella Guida per l'utente di AWS Direct Connect.

Crittografia in transito per i dati VMware di rete

Dopo l'implementazione dell'ambiente Amazon EVS, hai diverse opzioni per applicare la crittografia dei dati in transito a livello VCF: VMware

- VMware vDefend Distributed Firewall: consente di implementare una segmentazione di rete dettagliata e di applicare la crittografia tra macchine virtuali. TLS/SSL Per ulteriori informazioni, vedere Configurare le impostazioni di sicurezza per il firewall distribuito utilizzando l'interfaccia utente nella documentazione VCF. VMware
- data-in-transitCrittografia vSAN: può essere utilizzata per crittografare tutti i dati e i metadati tra gli host del cluster vSAN. Per ulteriori informazioni, vedere vSAN Data-In-Transit Encryption nella documentazione di vSAN VMware .
- Encrypted vSphere vMotion: protegge la riservatezza, l'integrità e l'autenticità dei dati trasferiti con vSphere vMotion. Per ulteriori informazioni, vedere Cos'è Encrypted vSphere vMotion nella documentazione di vSphere.

Gestione delle chiavi e dei segreti

Durante l'implementazione dell'ambiente Amazon EVS, Amazon EVS utilizza AWS Secrets Manager per creare, crittografare e archiviare segreti che contengono le credenziali VCF necessarie per installare e accedere ai dispositivi di gestione VMware VCF, oltre alla password root ESX. Amazon EVS elimina anche i segreti gestiti per tuo conto quando l'ambiente EVS viene eliminato. Per ulteriori informazioni, consulta Cosa c'è in un segreto di Secrets Manager nella Guida per l'utente di AWS Secrets Manager.

Secrets Manager utilizza la crittografia a busta con AWS KMS chiavi e chiavi dati per proteggere ogni valore segreto. La chiave AWS gestita predefinita per Secrets Manager viene utilizzata se non diversamente specificato. In alternativa, puoi specificare una chiave gestita dal cliente durante la creazione dell'ambiente per crittografare i tuoi segreti. Per ulteriori informazioni, vedere Crittografia e decrittografia segrete in AWS Secrets Manager nella Guida per l'utente di AWS Secrets Manager.

> **Note**
>
> Sono previsti costi di utilizzo aggiuntivi per le chiavi gestite dai clienti. La chiave AWS gestita predefinita viene fornita gratuitamente. Per ulteriori informazioni, consulta la sezione Prezzi nella Guida per l'utente di AWS Secrets Manager.

Amazon EVS non sincronizza le credenziali tra AWS Secrets Manager e il software VCF dopo la distribuzione. È tua responsabilità garantire che i segreti associati al tuo ambiente Amazon EVS siano mantenuti sincronizzati con le credenziali in SDDC Manager per evitare la scadenza della password VCF e la perdita di accesso al software VCF.

Amazon EVS non divulga segreti per tuo conto. Sei responsabile della rotazione dei segreti associati al tuo ambiente. Ti consigliamo vivamente di ruotare i tuoi segreti non appena l'ambiente viene creato e di implementare una pianificazione di rotazione per aggiornare i tuoi segreti a intervalli regolari. Per ulteriori informazioni sulla rotazione dei AWS segreti di Secrets Manager, vedete la funzione Rotation by Lambda nella Guida per l'utente di Secrets AWS Manager. Per ulteriori informazioni sulla gestione delle password VCF, consulta Gestione delle password nella documentazione di VMware Cloud Foundation.

Important

Amazon EVS non sincronizza le credenziali tra AWS Secrets Manager e il software VCF dopo la distribuzione. Se si utilizza AWS Secrets Manager dopo la distribuzione, è necessario mantenere sincronizzate le credenziali tra AWS Secrets Manager e SDDC Manager per evitare problemi di scadenza della password VCF. È possibile perdere l'accesso al software VCF se le credenziali di SDDC Manager non vengono mantenute aggiornate.

Note

Amazon EVS non fornisce una rotazione gestita dei segreti.

Note

L'utilizzo di una funzione Lambda per la rotazione segreta di AWS Secrets Manager comporta dei costi. Per ulteriori informazioni, consulta la sezione Prezzi nella Guida per l'utente di AWS Secrets Manager.

Riservatezza del traffico Internet

Amazon EVS utilizza un VPC fornito dal cliente per creare confini tra le risorse nell'ambiente Amazon EVS e controllare il traffico tra esse, la rete locale e Internet. Per ulteriori informazioni sulla Amazon

VPC sicurezza, consulta Garantire la privacy del traffico di rete nella Guida per l'utente. Amazon VPC Amazon VPC

Per impostazione predefinita, Amazon EVS crea sottoreti VLAN private durante la creazione dell'ambiente che negano l'accesso diretto a Internet. Per aggiungere un altro livello di sicurezza al tuo VPC, puoi creare un elenco di controllo degli accessi alla rete personalizzato per il tuo VPC con regole che limitano ulteriormente la connettività Internet. Per ulteriori informazioni, consulta Creare un ACL di rete per il tuo VPC nella Amazon VPC User Guide.

> **Important**
>
> I gruppi di sicurezza EC2 non funzionano su interfacce di rete elastiche collegate alle sottoreti VLAN di Amazon EVS. Per controllare il traffico da e verso le sottoreti VLAN di Amazon EVS, devi utilizzare una lista di controllo dell'accesso alla rete.

Se sei un amministratore NSX, puoi configurare le seguenti funzionalità di NSX per proteggere il traffico di rete:

- VMware vDefend Gateway Firewall: protegge il perimetro della rete, proteggendolo dalle minacce esterne (traffico nord-sud). Per ulteriori informazioni, vedere Aggiungere una politica e una regola del gateway firewall nella documentazione di NSX. VMware
- VMware vDefend Distributed Firewall: protegge dagli attacchi provenienti dall'interno di una rete interna (traffico est-ovest). Per ulteriori informazioni, vedere Aggiungere un firewall distribuito nella documentazione di NSX. VMware

Gestione delle identità e degli accessi per Amazon Elastic VMware Service

AWS Identity and Access Management (IAM) è uno strumento Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. IAM gli amministratori controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse di Amazon Elastic Service VMware (Amazon EVS). IAM è un software Servizio AWS che puoi utilizzare senza costi aggiuntivi.

Argomenti

- Autenticazione con identità
- Gestione dell'accesso tramite policy
- Come funziona Amazon EVS con IAM
- Esempi di policy basate sull'identità di Amazon EVS
- Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon EVS
- AWS politiche gestite per Amazon EVS
- Utilizzo di ruoli collegati ai servizi per Amazon EVS

Destinatari

Il modo in cui usi AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in Amazon EVS.

Utente del servizio: se utilizzi il servizio Amazon EVS per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più funzionalità di Amazon EVS per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso consente di richiedere le autorizzazioni corrette all'amministratore.

Se non riesci ad accedere a una funzionalità in Amazon EVS, consultathe section called "Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon EVS".

Amministratore del servizio: se sei responsabile delle risorse Amazon EVS della tua azienda, probabilmente hai pieno accesso ad Amazon EVS. È tuo compito determinare a quali funzionalità e risorse di Amazon EVS devono accedere gli utenti del servizio. Devi quindi inviare richieste all' IAM amministratore per modificare le autorizzazioni degli utenti del servizio. Consulta le informazioni contenute in questa pagina per comprendere i concetti di base di IAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM Amazon EVS, consultathe section called "Come funziona Amazon EVS con IAM".

IAM amministratore: se sei un IAM amministratore, potresti voler saperne di più su come scrivere politiche per gestire l'accesso ad Amazon EVS. Per visualizzare esempi di policy basate sull'identità di Amazon EVS che puoi utilizzare, consulta. IAMthe section called "Esempi di policy basate sull'identità di Amazon EVS"

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. È necessario autenticarsi (accedere a AWS) come utente root dell' AWS account o assumere un Utente IAM ruolo. IAM

È possibile accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center (IAM Identity Center) gli utenti, l'autenticazione Single Sign-On della tua azienda e le tue credenziali Google o Facebook sono esempi di identità federate. Quando accedi come identità federata, l'amministratore aveva precedentemente configurato la federazione delle identità utilizzando i ruoli. IAM Quando si accede AWS utilizzando la federazione, si assume indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al Console di gestione AWS o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'utente di AWS accesso.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta il processo di firma della versione 4 di Signature nella AWS Guida generale.

Indipendentemente dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta l'autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center (successore di AWS Single Sign-On) e l'utilizzo dell'autenticazione a più fattori (MFA) AWS nella Guida per l'utente IAM.

AWS account (utente root)

La prima volta che si crea un account Account AWS, si inizia con un'identità con accesso singolo che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente root dell' AWS account ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per l'elenco completo delle attività che richiedono l'accesso come utente root, consulta Attività che richiedono le credenziali dell'utente root nella Guida di riferimento per la gestione degli account.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le Servizi AWS credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per informazioni su IAM Identity Center, consulta Cos'è IAM Identity Center? nella Guida per l' AWS utente di IAM Identity Center (successore di AWS Single Sign-On).

Utenti IAM e gruppi

An Utente IAMè un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Laddove possibile, consigliamo di fare affidamento su credenziali temporanee anziché creare Utenti IAM utenti con credenziali a lungo termine come password e chiavi di accesso. Tuttavia, se hai casi d'uso specifici che richiedono credenziali a lungo termine Utenti IAM, ti consigliamo di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente IAM.

Un IAM gruppo è un'identità che specifica un insieme di. Utenti IAM Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni di set di utenti di grandi dimensioni. Ad esempio, è possibile assegnare un nome a un gruppo IAMAdminse concedere a tale gruppo le autorizzazioni per IAM amministrare le risorse.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali permanenti a lungo termine, ma i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un Utente IAM (anziché un ruolo) nella Guida per l'utente IAM.

IAM ruoli

Un IAM ruolo è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a una persona Utente IAM, ma non è associato a una persona specifica. È possibile assumere temporaneamente un IAM ruolo in Console di gestione AWS cambiando ruolo. Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi di utilizzo dei ruoli, consulta Using IAM roles nella IAM User Guide.

IAM i ruoli con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato - Per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. Centro identità IAM mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare le risorse alle quali le identità possono accedere dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center (successore di AWS Single Sign-On).
- Utente IAM Autorizzazioni temporanee: An Utente IAM può assumere il IAM ruolo di assumere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso su più account: puoi utilizzare un IAM ruolo per consentire a qualcuno (un responsabile fidato) di un altro account di accedere alle risorse del tuo account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per conoscere la differenza tra i ruoli e le politiche basate sulle risorse per l'accesso tra account diversi, consulta How IAM roles differiscono dalle policy basate sulle risorse nella IAM User Guide.
- Accesso tra servizi: alcuni utilizzano funzionalità in altri. Servizi AWS Servizi AWS Ad esempio, quando si effettua una chiamata in un servizio, è normale che quel servizio esegua applicazioni Amazon EC2 o in cui memorizzi oggetti. Amazon S3 Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, un ruolo di servizio oppure un ruolo collegato al servizio.
  - Autorizzazioni principali: quando utilizzi un ruolo Utente IAM o per eseguire azioni AWS, sei considerato un principale. Le policy concedono autorizzazioni a un'entità. Quando si utilizzano alcuni servizi, è possibile eseguire un'azione che attiva un'altra azione in un servizio diverso. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni.

- Ruolo di servizio: un ruolo di servizio è un IAM ruolo che un servizio assume per eseguire azioni per conto dell'utente. Un IAM amministratore può creare, modificare ed eliminare un ruolo di servizio dall'interno IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.
- Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'operazione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un IAM amministratore può visualizzare, ma non modificare le autorizzazioni per i ruoli collegati al servizio.

- Applicazioni in esecuzione Amazon EC2 : è possibile utilizzare un IAM ruolo per gestire le credenziali temporanee per le applicazioni in esecuzione su un' Amazon EC2 istanza e che AWS CLI effettuano richieste API. AWS Ciò è preferibile alla memorizzazione delle chiavi di accesso all'interno dell' Amazon EC2 istanza. Per assegnare un AWS ruolo a un' Amazon EC2 istanza e renderlo disponibile per tutte le sue applicazioni, create un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull' Amazon EC2 istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta Usare un IAM ruolo per concedere le autorizzazioni alle applicazioni in esecuzione su Amazon EC2 istanze nella Guida per l'utente IAM.

Per sapere se utilizzare IAM i ruoli, consulta Quando creare un IAM ruolo (anziché un utente) nella Guida per l'utente IAM.

Gestione dell'accesso tramite policy

Puoi controllare l'accesso AWS creando policy e associandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per maggiori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente di IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

Ogni IAM entità (utente o ruolo) inizia senza autorizzazioni. Di default, gli utenti non possono eseguire alcuna operazione, neppure modificare la propria password. Per autorizzare un utente a eseguire

operazioni, un amministratore deve allegare una policy di autorizzazioni a tale utente. In alternativa, l'amministratore può aggiungere l'utente a un gruppo che dispone delle autorizzazioni desiderate. Quando un amministratore concede le autorizzazioni a un gruppo, a tutti gli utenti di quel gruppo vengono concesse tali autorizzazioni.

IAM le politiche definiscono le autorizzazioni per un'azione indipendentemente dal metodo utilizzato per eseguire l'operazione. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' Console di gestione AWS AWS CLI, dall'o dall' AWS API.

Policy basate sull'identità

Le politiche basate sull'identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità, ad esempio un ruolo o un gruppo Utente IAM. Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per scoprire come creare una policy basata sull'identità, consulta Creating policies nella IAM User Guide. IAM

Le policy basate sull'identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le policy gestite sono policy autonome che puoi allegare a più utenti, gruppi e ruoli all'interno del tuo. Account AWS Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente IAM.

Policy basate su risorse

Le politiche basate sulle risorse sono documenti di policy JSON allegati a una risorsa come un bucket. Amazon S3 Gli amministratori di servizio possono utilizzare queste policy per definire quali operazioni può eseguire un principal specificato (membro, utente, ruolo account) su quella risorsa e in quali condizioni. Le policy basate su risorse sono policy inline. Non esistono policy basate su risorse gestite.

Elenchi di controllo degli accessi () ACLs

Le liste di controllo degli accessi (ACLs) sono un tipo di politica che controlla a quali responsabili (membri dell'account, utenti o ruoli) sono autorizzati ad accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON. Amazon S3 AWS WAF, e Amazon VPC sono esempi di servizi che supportano. ACLs Per ulteriori informazioni ACLs, consulta la panoramica dell'Access Control List (ACL) nella Amazon Simple Storage Service Developer Guide.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai più tipi di policy comuni.

- Limiti delle autorizzazioni: un limite di autorizzazioni è una funzionalità avanzata in cui si impostano le autorizzazioni massime che una politica basata sull'identità può concedere a un'entità (o ruolo). IAM Utente IAM È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate sull'identità dell'entità e i rispettivi limiti delle autorizzazioni. Le policy basate sulle risorse che specificano l'utente o il ruolo nel campo `Principal` non sono interessate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità nella Guida per l'utente IAM. IAM
- Policy di controllo del servizio (SCPs): SCPs sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più di proprietà dell' Account AWS azienda. Se abiliti tutte le funzionalità di un'organizzazione, puoi applicare le politiche di controllo del servizio (SCPs) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità negli account dei membri, incluso ogni AWS utente root dell'account. Per ulteriori informazioni su Organizations and SCPs, consulta How SCPs work nella AWS Organizations User Guide.
- Policy di sessione - Le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate sull'identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando a una richiesta si applicano più tipi di policy, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire o meno una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

Come funziona Amazon EVS con IAM

Prima di utilizzare IAM per gestire l'accesso ad Amazon EVS, scopri quali IAM funzionalità sono disponibili per l'uso con Amazon EVS.

IAM funzionalità	Supporto Amazon EVS
the section called “Policy basate sull'identità per Amazon EVS”	Sì
the section called “Policy basate sulle risorse all'interno di Amazon EVS”	No
the section called “Azioni politiche per Amazon EVS”	Sì
the section called “Risorse relative alle policy per Amazon EVS”	Parziale
the section called “Chiavi relative alle condizioni delle politiche per Amazon EVS”	Sì
the section called “Elenchi di controllo degli accessi (ACLs) in Amazon EVS”	No
the section called “Controllo degli accessi basato sugli attributi (ABAC) con Amazon EVS”	Sì
the section called “Utilizzo di credenziali temporanee con Amazon EVS”	Sì
the section called “Sessioni di accesso diretto per Amazon EVS”	Sì
the section called “Ruoli di servizio per Amazon EVS”	No
the section called “Ruoli collegati ai servizi per Amazon EVS”	Sì

Per avere una panoramica di alto livello su come Servizi AWS funzionano Amazon EVS e altri IAM, consulta Servizi AWS la sezione Working with IAM nella IAM User Guide.

Policy basate sull'identità per Amazon EVS

Supporta le policy basate sull'identità: sì

Le policy basate sull'identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente di IAM.

Con le politiche IAM basate sull'identità, puoi specificare azioni e risorse consentite o negate, nonché le condizioni in base alle quali le azioni sono consentite o negate. Non è possibile specificare il principale in una politica basata sull'identità perché si applica all'utente o al ruolo a cui è associata. Per maggiori informazioni su tutti gli elementi utilizzati in una policy JSON, consulta il riferimento agli elementi della policy IAM JSON nella IAM User Guide.

Esempi di policy basate sull'identità per Amazon EVS

Per visualizzare esempi di policy basate sull'identità di Amazon EVS, consulta. the section called "Esempi di policy basate sull'identità di Amazon EVS"

Policy basate sulle risorse all'interno di Amazon EVS

Supporta le policy basate su risorse: no

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy di bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. In una policy basata sulle risorse è obbligatorio specificare un'entità principale. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, è possibile specificare un intero account o entità IAM in un altro account come entità principale in una policy basata sulle risorse. L'aggiunta di un'entità principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un amministratore IAM dell'account affidabile deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere

alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate sull'identità. Per ulteriori informazioni, consulta Cross Account Resource Access in IAM nella IAM User Guide.

Azioni politiche per Amazon EVS

Supporta azioni Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'`Action`elemento di una policy IAM basata sull'identità descrive l'azione o le azioni specifiche che saranno consentite o negate dalla policy. Le azioni politiche in genere hanno lo stesso nome dell'operazione API associata AWS . L'operazione viene utilizzata in una policy per concedere le autorizzazioni di eseguire l'operazione associata.

Le azioni politiche in Amazon EVS utilizzano il seguente prefisso prima dell'azione:. `evs:` Ad esempio, per concedere a qualcuno l'autorizzazione a creare un ambiente con il funzionamento dell'`CreateEnvironment`API Amazon EVS, includi l'`evs:CreateEnvironment`azione nella sua politica. Le istruzioni della policy devono includere un elemento `Action` o `NotAction`. Amazon EVS definisce il proprio set di azioni che descrivono le attività che è possibile eseguire con questo servizio.

Per specificare più azioni in una sola istruzione, separa ciascuna di esse con una virgola come mostrato di seguito:

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

È possibile specificare più azioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le azioni che iniziano con la parola `List`, includi la seguente azione:

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

Per visualizzare un elenco di azioni Amazon EVS, consulta Actions Defined by Amazon EVS nel Service Authorization Reference.

Risorse relative alle policy per Amazon EVS

Supporto risorse policy: Parziale

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Le istruzioni devono includere un elemento `Resource` o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). È possibile eseguire questa operazione per operazioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

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

Per visualizzare un elenco dei tipi di risorse Amazon EVS e relativi ARNs, consulta Risorse definite da Amazon Elastic VMware Service nel Service Authorization Reference. Per sapere con quali azioni puoi specificare l'ARN di ogni risorsa, consulta Azioni definite da Amazon Elastic VMware Service.

Alcune azioni dell'API Amazon EVS supportano più risorse. Ad esempio, è possibile fare riferimento a più ambienti quando si chiama l'azione `ListEnvironments` API. Per specificare più risorse in una singola istruzione, separale ARNs con virgole.

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

Ad esempio, la risorsa di ambiente Amazon EVS ha il seguente ARN:

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

Per specificare gli ambienti `my-environment-1` e `my-environment-2` nella tua dichiarazione, usa il seguente esempio: ARNs

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

Per specificare tutti gli ambienti che appartengono a un account specifico, usa il carattere jolly (*):

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

Chiavi relative alle condizioni delle politiche per Amazon EVS

Supporta le chiavi di condizione delle policy specifiche del servizio: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'`Condition`elemento (o `Condition` blocco) consente di specificare le condizioni in cui un'istruzione è valida. L'elemento `Condition` è facoltativo. È possibile compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition` in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND` logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'0Roperazione logica. Tutte le condizioni devono essere soddisfatte prima che vengano concesse le autorizzazioni della dichiarazione.

È possibile anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi concedere l' Utente IAM autorizzazione ad accedere a una risorsa solo se è contrassegnata con Utente IAM il suo nome. Per ulteriori informazioni, consulta gli elementi delle IAM policy: variabili e tag nella IAM User Guide.

Amazon EVS definisce il proprio set di chiavi di condizione e supporta anche l'utilizzo di alcune chiavi di condizione globali. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Tutte Amazon EC2 le azioni supportano i tasti `aws:RequestedRegion` and `ec2:Region` condition. Per ulteriori informazioni, consulta Esempio: limitazione dell'accesso a una regione specifica.

Per visualizzare un elenco di chiavi di condizione di Amazon EVS, consulta Condition Keys for Amazon EVS nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, consulta Azioni definite da Amazon EVS.

Elenchi di controllo degli accessi (ACLs) in Amazon EVS

Supporti ACLs: No

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

Controllo degli accessi basato sugli attributi (ABAC) con Amazon EVS

Supporta ABAC (tag nelle policy): sì

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. Puoi allegare tag a entità IAM (utenti o ruoli) e a molte AWS risorse. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. Quindi si progettano politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag sulla risorsa a cui sta tentando di accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Puoi allegare tag alle risorse Amazon EVS o passare i tag in una richiesta ad Amazon EVS. Per controllare l'accesso basato su tag, fornire informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/<key-name>`, `aws:RequestTag/<key-name>` o `aws:TagKeys`. Per ulteriori informazioni sulle azioni con cui puoi utilizzare i tag nelle chiavi di condizione, consulta Actions defined by Amazon EVS nel Service Authorization Reference.

Utilizzo di credenziali temporanee con Amazon EVS

Supporta le credenziali temporanee: sì

Alcune Servizi AWS non funzionano quando accedi utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta Servizi AWS la sezione relativa alla funzionalità di IAM nella IAM User Guide.

Stai utilizzando credenziali temporanee se accedi Console di gestione AWS utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedi AWS utilizzando il link Single Sign-On (SSO) della tua azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando si accede alla console come utente e poi si cambia ruolo. Per maggiori informazioni sullo scambio dei ruoli, consulta Passaggio da un ruolo utente a un ruolo IAM (console) nella Guida per l'utente di IAM.

È possibile creare manualmente credenziali temporanee utilizzando l'API or. AWS CLI AWS È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare

dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per maggiori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

Sessioni di accesso diretto per Amazon EVS

Supporta l'inoltro delle sessioni di accesso (FAS): sì

Quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.

Ruoli di servizio per Amazon EVS

Supporta i ruoli di servizio: no

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente IAM.

Ruoli collegati ai servizi per Amazon EVS

Supporta i ruoli collegati ai servizi: Sì

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'operazione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati al servizio, ma non modificarle.

Per dettagli sulla creazione o la gestione di ruoli collegati ai servizi Amazon EVS, consulta. the section called "Uso di ruoli collegati ai servizi"

Esempi di policy basate sull'identità di Amazon EVS

Per impostazione predefinita, Utenti IAM i ruoli non dispongono dell'autorizzazione per creare o modificare risorse Amazon EVS. Inoltre, non possono eseguire attività utilizzando l' AWS API

Console di gestione AWS AWS CLI, o. Un IAM amministratore deve creare IAM politiche che concedano a utenti e ruoli l'autorizzazione a eseguire operazioni API specifiche sulle risorse specifiche di cui ha bisogno. L'amministratore deve quindi allegare tali politiche agli Utenti IAM o ai gruppi che richiedono tali autorizzazioni.

Per scoprire come creare una policy basata sull'identità IAM utilizzando questi esempi di documenti di policy JSON, consulta Creating policies using the JSON editor nella IAM User Guide.

Argomenti

- Best practice per le policy
- Utilizzo della console Amazon EVS
- Consentire agli utenti di visualizzare le loro autorizzazioni
- Crea e gestisci un ambiente Amazon EVS
- Ottieni ed elenca ambienti, host Amazon EVS e VLANs

Best practice per le policy

Le policy basate sull'identità determinano se qualcuno può creare, accedere o eliminare risorse Amazon EVS nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando si creano o modificano policy basate sull'identità, seguire queste linee guida e raccomandazioni:

- Inizia con le politiche AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni. AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per maggiori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente di IAM.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le IAM politiche, concedi solo le autorizzazioni necessarie per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegio minimo. Per ulteriori informazioni sull'utilizzo IAM per applicare le autorizzazioni, consulta Policies and permissions nella IAM User Guide. IAM
- Utilizza le condizioni nelle IAM policy per limitare ulteriormente l'accesso: puoi aggiungere una condizione alle tue policy per limitare l'accesso ad azioni e risorse. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando

SSL. È inoltre possibile utilizzare le condizioni per concedere l'accesso alle azioni di servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio CloudFormation. Per ulteriori informazioni, consulta IAM JSON Policy elements: condition nella IAM User Guide.

- IAM Access Analyzer Utilizzalo per convalidare le IAM policy per garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio delle IAM policy (JSON) e alle best practice. IAM IAM Access Analyzer fornisce più di 100 controlli delle politiche e consigli pratici per aiutarti a creare policy sicure e funzionali. Per ulteriori informazioni, consulta la convalida IAM Access Analyzer delle policy nella IAM User Guide.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che Utenti IAM richiede l'utilizzo di utenti root nel tuo account, attiva l'autenticazione a più fattori per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente IAM.

Utilizzo della console Amazon EVS

Per accedere alla console Amazon EVS, un principale IAM deve disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentire al responsabile di elencare e visualizzare i dettagli sulle risorse Amazon EVS presenti nel tuo. Account AWS Se crei una policy di basata su identità più restrittiva delle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per i principali associati a tale policy.

Per garantire che i tuoi responsabili IAM possano ancora utilizzare la console Amazon EVS, crea una policy con il tuo nome univoco, ad esempio. `AmazonEVSAdminPolicy` Allega la politica ai principali. Per ulteriori informazioni, consulta la sezione Aggiunta di autorizzazioni a un utente nella Guida per l'utente di IAM:

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

```
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/evs.amazonaws.com/
AWSServiceRoleForEVS",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "evs.amazonaws.com"
                }
            }
        }
    ]
}
```

Non è necessario consentire autorizzazioni minime per la console per gli utenti che effettuano chiamate solo verso AWS CLI o l'API. AWS Al contrario, è possibile accedere solo alle operazioni che soddisfano l'operazione API che stai cercando di eseguire.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra come è possibile creare una politica che Utenti IAM consenta di visualizzare le politiche in linea e gestite allegate alla loro identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando l'API o a livello di codice. AWS CLI AWS

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
```

```
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Crea e gestisci un ambiente Amazon EVS

Questa policy di esempio include le autorizzazioni necessarie per creare ed eliminare un ambiente Amazon EVS e aggiungere o eliminare host dopo la creazione dell'ambiente.

Puoi sostituirlo Regione AWS con Regione AWS quello in cui desideri creare un ambiente. Se il tuo account dispone già del ruolo `AWSServiceRoleForAmazonEVS`, puoi rimuovere l'azione `iam:CreateServiceLinkedRole` dalla policy. Se hai mai creato un ambiente Amazon EVS nel tuo account, esiste già un ruolo con queste autorizzazioni, a meno che tu non lo abbia eliminato.

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ReadOnlyDescribeActions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeHosts",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeAddresses",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeSubnets",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeInstances",
                "ec2:DescribeRouteServers",
                "ec2:DescribeRouteServerEndpoints",
```

```
                "ec2:DescribeRouteServerPeers",
                "ec2:DescribePlacementGroups",
                "ec2:DescribeVolumes",
                "ec2:DescribeSecurityGroups",
                "support:DescribeServices",
                "support:DescribeSupportLevel",
                "servicequotas:GetServiceQuota",
                "servicequotas:ListServiceQuotas"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ModifyNetworkInterfaceStatement",
            "Effect": "Allow",
            "Action": [
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "ModifyNetworkInterfaceStatementForSubnetAssociation",
            "Effect": "Allow",
            "Action": [
                "ec2:ModifyNetworkInterfaceAttribute"
            ],
            "Resource": "arn:aws:ec2:*:*:subnet/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "CreateNetworkInterfaceWithTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface"
            ],
```

```
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "Null": {
                    "aws:RequestTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "CreateNetworkInterfaceAdditionalResources",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:security-group/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "TagOnCreateEC2Resources",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*",
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ec2:*:*:volume/*",
                "arn:aws:ec2:*:*:subnet/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": [
                        "CreateNetworkInterface",
                        "RunInstances",
                        "CreateSubnet",
                        "CreateVolume"
```

```
                ]
            },
            "Null": {
                "aws:RequestTag/AmazonEVSManaged": "false"
            }
        }
    },
    {
        "Sid": "DetachNetworkInterface",
        "Effect": "Allow",
        "Action": [
            "ec2:DetachNetworkInterface"
        ],
        "Resource": [
            "arn:aws:ec2:*:*:network-interface/*",
            "arn:aws:ec2:*:*:instance/*"
        ],
        "Condition": {
            "Null": {
                "aws:ResourceTag/AmazonEVSManaged": "false"
            }
        }
    },
    {
        "Sid": "RunInstancesWithTag",
        "Effect": "Allow",
        "Action": [
            "ec2:RunInstances"
        ],
        "Resource": [
            "arn:aws:ec2:*:*:instance/*",
            "arn:aws:ec2:*:*:volume/*"
        ],
        "Condition": {
            "Null": {
                "aws:RequestTag/AmazonEVSManaged": "false"
            }
        }
    },
    {
        "Sid": "RunInstancesWithTagResource",
        "Effect": "Allow",
        "Action": [
            "ec2:RunInstances"
```

```
            ],
            "Resource": [
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "RunInstancesWithoutTag",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:image/*",
                "arn:aws:ec2:*:*:security-group/*",
                "arn:aws:ec2:*:*:key-pair/*",
                "arn:aws:ec2:*:*:placement-group/*"
            ]
        },
        {
            "Sid": "TerminateInstancesWithTag",
            "Effect": "Allow",
            "Action": [
                "ec2:TerminateInstances",
                "ec2:ModifyInstanceAttribute"
            ],
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "CreateSubnetWithTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSubnet"
            ],
```

```
            "Resource": [
                "arn:aws:ec2:*:*:subnet/*"
            ],
            "Condition": {
                "Null": {
                    "aws:RequestTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "CreateSubnetWithoutTagForExistingVPC",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSubnet"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:vpc/*"
            ]
        },
        {
            "Sid": "DeleteSubnetWithTag",
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteSubnet"
            ],
            "Resource": "arn:aws:ec2:*:*:subnet/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "VolumeDeletion",
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteVolume"
            ],
            "Resource": "arn:aws:ec2:*:*:volume/*",
             "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
```

```
        },
        {
            "Sid": "VolumeDetachment",
            "Effect": "Allow",
            "Action": [
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "RouteServerAccess",
            "Effect": "Allow",
            "Action": [
                "ec2:GetRouteServerAssociations"
            ],
            "Resource": "arn:aws:ec2:*:*:route-server/*"

        },
        {
            "Sid": "EVSServiceLinkedRole",
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/evs.amazonaws.com/
AWSServiceRoleForEVS",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "evs.amazonaws.com"
                }
            }
        },
        {
            "Sid": "SecretsManagerCreateWithTag",
            "Effect": "Allow",
            "Action": [
```

```
                "secretsmanager:CreateSecret"
            ],
            "Resource": "arn:aws:secretsmanager:*:*:secret:*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/AmazonEVSManaged": "true"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AmazonEVSManaged"
                    ]
                }
            }
        },
        {
            "Sid": "SecretsManagerTagging",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:TagResource"
            ],
            "Resource": "arn:aws:secretsmanager:*:*:secret:*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/AmazonEVSManaged": "true",
                    "aws:ResourceTag/AmazonEVSManaged": "true"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AmazonEVSManaged"
                    ]
                }
            }
        },
        {
            "Sid": "SecretsManagerOps",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:DeleteSecret",
                "secretsmanager:GetSecretValue",
                "secretsmanager:UpdateSecret"
            ],
            "Resource": "arn:aws:secretsmanager:*:*:secret:*",
            "Condition": {
                "Null": {
```

```
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "SecretsManagerRandomPassword",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetRandomPassword"
            ],
            "Resource": "*"
        },
        {
            "Sid": "EVSPermissions",
            "Effect": "Allow",
            "Action": [
                "evs:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KMSKeyAccessInConsole",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey"
            ],
            "Resource": "arn:aws:kms:*:*:key/*"
        },

        {
            "Sid": "KMSKeyAliasAccess",
            "Effect": "Allow",
            "Action": [
                "kms:ListAliases"
            ],
            "Resource": "*"
        }
    ]
}
```

Ottieni ed elenca ambienti, host Amazon EVS e VLANs

Questa policy di esempio include le autorizzazioni minime richieste a un amministratore per ottenere ed elencare tutti gli ambienti Amazon EVS, gli host e VLANs all'interno di un determinato account in us-east-2. Regione AWS

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

Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon EVS

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con Amazon EVS e. IAM

Argomenti

- AccessDeniedException
- Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse Amazon EVS

AccessDeniedException

Se ricevi un messaggio `AccessDeniedException` quando chiami un'operazione AWS API, le credenziali principali IAM che stai utilizzando non dispongono delle autorizzazioni necessarie per effettuare quella chiamata.

```
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
```

Nel messaggio di esempio precedente, l'utente non dispone delle autorizzazioni per chiamare l'operazione dell'`CreateEnvironment`API Amazon EVS. Per fornire le autorizzazioni di amministratore di Amazon EVS a un principale IAM, consulta. the section called "Esempi di policy basate sull'identità di Amazon EVS"

Per informazioni più generali su IAM, consulta Controllare l'accesso alle AWS risorse utilizzando le policy nella IAM User Guide.

Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse Amazon EVS

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche per consentire alle persone di accedere alle tue risorse.

Per maggiori informazioni, consulta gli argomenti seguenti:

- Per sapere se Amazon EVS supporta queste funzionalità, consultathe section called "Come funziona Amazon EVS con IAM".
- Per scoprire come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta Fornire l'accesso a un Utente IAM altro Account AWS utente di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terzi nella Guida per l'utente IAM.
- Per capire come fornire l'accesso tramite la federazione delle identità, consulta Fornire accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente di IAM.
- Per scoprire la differenza tra l'utilizzo dei ruoli e delle politiche basate sulle risorse per l'accesso tra account diversi, consulta How IAM roles differiscono dalle policy basate sulle risorse nella IAM User Guide.

AWS politiche gestite per Amazon EVS

Una politica AWS gestita è una politica autonoma creata e amministrata da. AWS AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Si consiglia pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i propri casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti. Per ulteriori informazioni, consulta le politiche AWS gestite nella Guida IAM per l'utente.

AWS politica gestita: Amazon EVSService RolePolicy

Non è possibile allegare `AmazonEVSServiceRolePolicy` alle entità IAM. Questa policy è associata a un ruolo collegato al servizio che consente ad Amazon EVS di eseguire azioni per tuo conto. Per ulteriori informazioni, consulta the section called "Uso di ruoli collegati ai servizi". Quando crei un ambiente utilizzando un principale IAM che dispone dell'`iam:CreateServiceLinkedRole`autorizzazione, il ruolo `AWSServiceRoleforAmazonEVS` collegato al servizio viene creato automaticamente per te con questa policy associata.

Questa policy consente al ruolo `AWSServiceRoleForAmazonEVS` collegato al servizio di chiamare Servizi AWS per tuo conto.

Dettagli delle autorizzazioni

Questa politica include le seguenti autorizzazioni che consentono ad Amazon EVS di completare le seguenti attività.

- `ec2`- Scopri i componenti di rete VPC, tra cui sottoreti e. VPCs Crea, modifica, etichetta ed elimina interfacce di rete elastiche utilizzate per stabilire una connessione persistente tra Amazon EVS e l'appliance SDDC Manager di VMware Virtual Cloud Foundation (VCF) nella tua sottorete VPC. Questa connettività è necessaria per Amazon EVS per distribuire, gestire e monitorare l'implementazione VCF.
- `ec2`- Elimina le istanze EC2 create da Amazon EVS quando effettui una richiesta di eliminazione di un host EVS. Descrivi e modifica gli attributi delle istanze EC2 in modo che la chiusura e l'interruzione della protezione predefinite dell'istanza EC2 possano essere disabilitate, se necessario, per supportare l'eliminazione degli host EVS.

- `ec2`- Gestisci i volumi EBS per l'installazione e la pulizia di Cloud Builder. Durante la creazione dell'ambiente, Cloud Builder viene installato su uno degli host distribuiti da Amazon EVS per eseguire modifiche alla configurazione VCF. Al termine, Amazon EVS rimuove Cloud Builder scollegando ed eliminando il volume EC2 su cui è archiviato.
- `ec2`- Elimina le sottoreti VLAN EVS per tuo conto se richiedi l'eliminazione dell'ambiente.
- `secretsmanager`- Elimina le password VCF che Amazon EVS crea e archivia in AWS Secrets Manager durante la creazione dell'ambiente. Amazon EVS elimina tutti i segreti che il servizio crea nel tuo account se la creazione dell'ambiente non riesce o se richiedi l'eliminazione dell'ambiente. Recupera le credenziali vCenter da Secrets AWS Manager quando configuri un connettore vCenter fornendo un ARN segreto. L'autorizzazione è soggetta a una condizione di tag di risorsa `EvsAccess=true` per garantire che Amazon EVS acceda solo ai segreti etichettati esplicitamente per l'accesso ad Amazon EVS vCenter.
- `kms`- Decrittografa i segreti e descrivi le chiavi KMS quando le credenziali vCenter archiviate in Secrets Manager sono crittografate con chiavi KMS. L'autorizzazione è soggetta a una condizione di tag di risorsa `EvsAccess=true` per garantire che Amazon EVS acceda solo alle chiavi KMS etichettate esplicitamente per l'accesso a vCenter.
- `cloudwatch`- Pubblica i parametri di AWS utilizzo CloudWatch per le risorse Amazon EVS con quote.

Per visualizzare maggiori dettagli sulla policy, inclusa l'ultima versione del documento sulla policy JSON, consulta Amazon EVSService RolePolicy nella AWS Managed Policy Reference Guide.

Aggiornamenti di Amazon EVS alle politiche AWS gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite per Amazon EVS da quando questo servizio ha iniziato a tracciare queste modifiche. Per gli avvisi automatici sulle modifiche apportate alla pagina, iscriviti al feed RSS alla pagina Cronologia dei documenti.

Modifica	Descrizione	Data
Amazon EVSService RolePolicy — Politica aggiornata	Amazon EVS ha aggiornato la policy per consentire al servizio di recuperare le credenziali vCenter da Secrets AWS Manager e di decrittografare i segreti crittografati	23 marzo 2026

Modifica	Descrizione	Data
	con chiavi KMS. Per ulteriori informazioni, consulta the section called "AWS politica gestita: Amazon EVSService RolePolicy".	
Amazon EVSService RolePolicy — Politica aggiornata	Amazon EVS ha aggiornato la policy per aggiungere funzionalità complete di gestione delle risorse, tra cui la gestione delle istanze EC2, le operazioni sui volumi EBS e l'integrazione di AWS Secrets Manager. Per ulteriori informazioni, consulta the section called "AWS politica gestita: Amazon EVSService RolePolicy".	14 agosto 2025
Amazon EVSService RolePolicy — Politica aggiornata	Amazon EVS ha aggiornato la policy per consentire al servizio di eliminare le sottoreti VLAN EVS e di pubblicare i parametri di utilizzo di Amazon EVS su. CloudWatch Per ulteriori informazioni, consulta the section called "AWS politica gestita: Amazon EVSService RolePolicy".	14 luglio 2025

Modifica	Descrizione	Data
Amazon EVSService RolePolicy — Aggiunta una nuova politica	Amazon EVS ha aggiunto una nuova policy che consente al servizio di connettersi a una sottorete VPC nell'account del cliente. Questa connessione è necessaria per la funzionalità del servizio. Per ulteriori informazioni, consulta the section called "AWS politica gestita: Amazon EVSService RolePolicy".	9 giugno 2025
Amazon EVS ha iniziato a tracciare le modifiche	Amazon EVS ha iniziato a tracciare le modifiche per le sue politiche AWS gestite.	9 giugno 2025

Utilizzo di ruoli collegati ai servizi per Amazon EVS

Amazon Elastic VMware Service utilizza ruoli AWS collegati al servizio Identity and Access Management (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM collegato direttamente ad Amazon EVS. I ruoli collegati ai servizi sono predefiniti da Amazon EVS e includono tutte le autorizzazioni richieste dal servizio per chiamare altri AWS servizi per tuo conto.

Un ruolo collegato al servizio semplifica la configurazione di Amazon EVS perché non è necessario aggiungere manualmente le autorizzazioni necessarie. Amazon EVS definisce le autorizzazioni dei suoi ruoli collegati ai servizi e, se non diversamente definito, solo Amazon EVS può assumerne i ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere allegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato al servizio solo dopo avere eliminato le risorse correlate. In questo modo proteggi le tue risorse Amazon EVS perché non puoi rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta Servizi AWS che funzionano con IAM e cerca i servizi che riportano Yes (Sì) nella colonna Service-linked roles (Ruoli

collegati ai servizi). Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni di ruolo collegate ai servizi per Amazon EVS

Amazon EVS utilizza il ruolo collegato al servizio denominato. `AWSServiceRoleForAmazonEVS` Il ruolo consente ad Amazon EVS di gestire gli ambienti del tuo account. La policy allegata consente al ruolo di gestire le seguenti risorse: interfacce di rete elastiche EVS, sottoreti VLAN EVS, host EVS e metriche. VPCs CloudWatch

Ai fini dell'assunzione del ruolo, il ruolo collegato al servizio `AWSServiceRoleForAmazonEVS` considera attendibili i seguenti servizi:

- `evs.amazonaws.com`

La politica di autorizzazione dei ruoli consente ad Amazon EVS di completare le seguenti azioni sulle risorse specificate:

- AmazonEVSServiceRolePolicy

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato al servizio è necessario configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente IAM.

Creazione di un ruolo collegato ai servizi per Amazon EVS

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando crei un ambiente nella AWS CLI o nell' AWS API, Amazon EVS crea il ruolo collegato al servizio per te. Console di gestione AWS

Se elimini questo ruolo collegato al servizio, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando crei un ambiente, Amazon EVS crea nuovamente il ruolo collegato ai servizi per te.

Modifica di un ruolo collegato ai servizi per Amazon EVS

Amazon EVS non consente di modificare il ruolo collegato al `AWSServiceRoleForAmazonEVS` servizio. Dopo avere creato un ruolo collegato al servizio, non sarà possibile modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione

utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato al servizio nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato al servizio per Amazon EVS

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato ai servizi prima di poterlo eliminare manualmente.

Pulizia di un ruolo collegato ai servizi

Prima di utilizzare IAM; per eliminare un ruolo collegato al servizio, è necessario prima rimuovere qualsiasi risorsa utilizzata dal ruolo. Per informazioni sulla procedura per eliminare un ambiente Amazon EVS con host, consultathe section called "Eliminare gli host e l'ambiente Amazon EVS".

> **Note**
>
> Se il servizio Amazon EVS utilizza il ruolo quando tenti di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Eliminazione manuale del ruolo collegato ai servizi

Utilizza la console IAM, la AWS CLI o l' AWS API per eliminare il ruolo collegato al `AWSServiceRoleForAmazonEVS` servizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente IAM.

Regioni supportate per i ruoli collegati ai servizi Amazon EVS

Amazon EVS supporta l'utilizzo di ruoli collegati al servizio in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta gli endpoint e le quote di Amazon Elastic VMware Service nella AWS General Reference Guide.

Resilienza in Amazon EVS

L'infrastruttura AWS globale è costruita attorno Regioni AWS a zone di disponibilità. Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate, collegate tramite reti a bassa

latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità è possibile progettare e gestire applicazioni e database che eseguono automaticamente il failover tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

Gli ambienti Amazon EVS sono disponibili in un'unica zona di AWS disponibilità. Per garantire l'elevata disponibilità dell'infrastruttura Amazon EVS Single-AZ, Amazon EVS offre le seguenti funzionalità:

> **Note**
>
> Al momento Amazon EVS supporta solo implementazioni Single-AZ.

- Amazon EVS supporta l'uso di AWS Elastic Disaster Recovery per automatizzare il backup e il ripristino dei dati.
- Amazon EVS implementa un cluster Active/Standby NSX Edge con due nodi NSX Edge per requisiti VCF. I nodi NSX Edge vengono eseguiti su host diversi per garantire un'elevata disponibilità e consentire un failover rapido nel raro caso in cui un nodo NSX Edge si guasti.
- Amazon EVS implementa un ambiente minimo di quattro host ESX, richiesto da VCF. È possibile aggiungere host aggiuntivi dopo l'implementazione. Si tratta di un requisito di VMware progettazione per garantire il corretto quorum di vSAN e mantenere la disponibilità durante le operazioni di manutenzione e i guasti dell'host. Per ulteriori informazioni, vedere vSphere Cluster Design for VMware Cloud Foundation nella documentazione di VMware Cloud Foundation.
- Amazon EVS supporta l'uso di un gruppo di posizionamento delle EC2 partizioni o di un gruppo di posizionamento del cluster per gli EC2 host. Il gruppo di posizionamento delle partizioni distribuisce le EC2 istanze su partizioni logiche in modo tale che i gruppi di istanze in una partizione non condividano l'hardware sottostante con gruppi di istanze in partizioni diverse. Questa strategia aiuta a ridurre la probabilità di guasti hardware correlati per carichi di lavoro distribuiti di grandi dimensioni. I cluster placement group vengono utilizzati per collocare le EC2 istanze all'interno dello stesso rack fisico per garantire una bassa latenza. Per ulteriori informazioni, consulta Partition Placement groups nella Guida per l'utente. Amazon EC2

Per ulteriori informazioni su AWS regioni e zone di disponibilità, vedere AWS Global Infrastructure.

VMware resilienza dei componenti

I clienti Amazon EVS sono responsabili della configurazione dei VMware componenti in esecuzione su Amazon EVS per garantire l'elevata disponibilità delle macchine virtuali (VMs) e la resilienza del carico di lavoro.

Amazon EVS supporta le seguenti funzionalità di resilienza di VMware Cloud Foundation (VCF):

- Replica vSphere: fornisce la replica asincrona basata su host per scopi di disaster recovery e migrazione dei carichi di lavoro. VMs Per ulteriori informazioni, vedere How vSphere Replication Works nella documentazione di vSphere VMware Replication.
- Protezione dei dati vSAN: consente di ripristinare rapidamente i guasti operativi VMs dovuti agli attacchi ransomware, utilizzando istantanee native archiviate localmente nel cluster vSAN. Per ulteriori informazioni, vedere Using vSAN Data Protection nella documentazione di vSAN.
- vSphere HA: fornisce il failover automatico VMs in caso di guasto dell'host. Per ulteriori informazioni, vedere High Availability Design for vCenter Server for VMware Cloud Foundation nella documentazione VCF.
- vSphere Fault Tolerance (FT): fornisce la disponibilità continua per le applicazioni mission critical VMs creando e gestendo un'altra macchina virtuale identica e sempre disponibile per sostituirla in caso di failover. Per ulteriori informazioni, vedere How Fault Tolerance Works nella documentazione di vSphere.
- vSAN Failure to Tolerate (FTT): un'impostazione vSAN che determina il numero di guasti dell'host che una macchina virtuale può sopportare prima di diventare inaccessibile. Questo definisce il livello di ridondanza e tolleranza agli errori per le macchine virtuali all'interno del cluster vSAN. Per ulteriori informazioni, vedere Tolerate Additional Failures with Fault Domain in vSAN Cluster nella documentazione di vSAN.

Utilizzo di Amazon EVS con altri servizi AWS

Amazon EVS è integrato con altri Servizi AWS per fornire soluzioni aggiuntive. Questo argomento identifica alcuni dei servizi con cui Amazon EVS collabora per aggiungere funzionalità.

Argomenti

Crea risorse Amazon EVS con AWS CloudFormation

Amazon EVS è integrato con AWS CloudFormation, un servizio che ti aiuta a modellare e configurare AWS le tue risorse in modo da poter dedicare meno tempo alla creazione e alla gestione delle risorse e dell'infrastruttura. Crei un modello che descrive tutte le AWS risorse che desideri, ad esempio un ambiente Amazon EVS, e AWS CloudFormation si occupa del provisioning e della configurazione di tali risorse per te.

Quando lo usi AWS CloudFormation, puoi riutilizzare il modello per configurare le risorse Amazon EVS in modo coerente e ripetuto. Descrivi le tue risorse una sola volta e poi fornisci le stesse risorse più e più volte in più regioni Account AWS .

Amazon EVS e modelli AWS CloudFormation

Per fornire e configurare risorse per Amazon EVS e i servizi correlati, devi conoscere i AWS CloudFormation modelli. I modelli sono file di testo formattati in JSON o YAML. Questi modelli descrivono le risorse che desideri fornire nei tuoi AWS CloudFormation stack. Se non conosci JSON o YAML, puoi usare AWS CloudFormation Designer per iniziare a usare i modelli. AWS CloudFormation Per ulteriori informazioni, consulta Cos'è Designer? AWS CloudFormation nella Guida AWS CloudFormation per l'utente.

Amazon EVS supporta la creazione di ambienti in AWS CloudFormation. Per ulteriori informazioni, inclusi esempi di modelli JSON e YAML per i tuoi ambienti, consulta il riferimento ai tipi di risorse Amazon EVS nella Guida per l'utente. AWS CloudFormation

Scopri di più su AWS CloudFormation

Per ulteriori informazioni AWS CloudFormation, consulta le seguenti risorse:

- AWS CloudFormation
- AWS CloudFormation Guida per l'utente
- AWS CloudFormation Guida per l'utente dell'interfaccia a riga di comando

Esegui carichi di lavoro ad alte prestazioni con Amazon FSx for ONTAP NetApp

Amazon FSx for NetApp ONTAP è un servizio di storage che consente di avviare ed eseguire file system ONTAP completamente gestiti nel cloud. ONTAP è NetApp la tecnologia di file system che fornisce un set ampiamente adottato di funzionalità di accesso e gestione dei dati. FSx for ONTAP offre le funzionalità, le prestazioni e le API dei NetApp file system locali con l'agilità, la scalabilità e la semplicità di un servizio completamente gestito. AWS Per ulteriori informazioni, consulta la Guida per l'utente di FSx per ONTAP.

Amazon EVS supporta l'uso di Amazon FSx NetApp for ONTAP come datastore e come storage NFS/iSCSI connesso a ospiti per macchine virtuali VMware in esecuzione su Amazon EVS.

Funzionalità FSx for NetApp ONTAP supportate

Le seguenti funzionalità di FSx for NetApp ONTAP sono state convalidate per l'uso con Amazon EVS:

Funzionalità	Description
Datastore NFS v3 esterni	Monta volumi FSx for ONTAP come datastore NFS v3 per VMware vSphere su Amazon EVS.
Datastore NFS v4.1 esterni	Monta i volumi FSx for ONTAP come datastore NFS v4.1 per VMware vSphere su Amazon EVS, fornendo funzionalità di sicurezza e prestazioni avanzate rispetto a NFS v3.
Datastore NVMe esterni	Usa FSx for ONTAP come datastore NVMe-based esterno per VMware vSphere su Amazon EVS, offrendo storage a blocchi ad alte prestazioni per carichi di lavoro impegnativi.
Datastore iSCSI	Configura FSx for ONTAP come i SCSI-based datastore VMFS per VMware vSphere su Amazon EVS.

Funzionalità	Description
Guest-mounted Dischi iSCSI	Presenta le LUN iSCSI FSx for ONTAP direttamente alle macchine virtuali guest in esecuzione su Amazon EVS come storage connesso in-guest.
NetApp SnapCenter Plug-in per VMware vSphere (SCV)	Utilizzalo NetApp SnapCenter Plug-in per VMware vSphere per fornire operazioni di backup e ripristino coerenti con le applicazi oni per VM e datastore in esecuzione su Amazon EVS.
Distribuzione tramite EVS Expansion VLAN	Implementa i datastore esterni FSx for ONTAP utilizzando una VLAN di espansione Amazon EVS per il traffico di rete di storage dedicato, garantendo isolamento della rete e prestazioni migliorate.

Configurazione FSx per NetApp ONTAP come datastore NFS

La procedura seguente descrive in dettaglio i passaggi minimi necessari FSx per configurare NetApp ONTAP come datastore NFS per Amazon EVS utilizzando la FSx console e l'interfaccia client VMware vSphere in esecuzione su Amazon EVS.

Prerequisiti

Prima di utilizzare Amazon EVS con Amazon FSx for NetApp ONTAP, assicurati che le seguenti attività prerequisite siano state completate.

- Un ambiente Amazon EVS viene distribuito nel tuo Virtual Private Cloud (VPC). Per ulteriori informazioni, consulta Nozioni di base.
- Hai accesso al tuo client vSphere in esecuzione su Amazon EVS.
- Tu o il tuo amministratore di storage dovete disporre delle autorizzazioni necessarie per creare e gestire i FSx file system ONTAP nel vostro VPC. Per ulteriori informazioni, consulta Gestione delle identità e degli accessi per Amazon FSx for NetApp ONTAP.

Il tuo responsabile IAM dispone delle autorizzazioni appropriate per creare e gestire i FSx file system ONTAP nel tuo VPC. Per ulteriori informazioni, consulta the section called "Crea e gestisci un ambiente Amazon EVS".

Crea un file system FSx per ONTAP NetApp

1. Vai alla FSx console Amazon.
2. Scegliere Create file system (Crea file system).
3. Seleziona Amazon FSx per NetApp ONTAP.
4. Scegli Next (Successivo).
5. Seleziona Standard create.
6. Per Tipo di implementazione, seleziona un'opzione di implementazione Single-AZ.

> **Note**
>
> Al momento Amazon EVS supporta solo implementazioni Single-AZ.

7. Per la capacità di archiviazione SSD, specificare 1024 GiB.
8. Per la capacità di trasmissione, scegli Specificare la capacità di trasmissione. Scegli almeno 512 MB/s per Single-AZ 1 o almeno 768 MB/s per Single-AZ 2.
9. Seleziona il VPC Amazon EVS con connettività alle sottoreti VLAN Amazon EVS.
10. Seleziona un gruppo di sicurezza che consenta tutto il traffico NFS necessario FSx per ONTAP alla sottorete VLAN di gestione dell'host VMkernel Amazon EVS.
11. Seleziona la sottorete di accesso al servizio Amazon EVS in cui verrà distribuito il file system. Per ulteriori informazioni, consulta the section called "Sottorete di accesso al servizio".
12. Per Junction path, specificare un nome significativo `/vol1` per identificare questo volume in vSphere.
13. Nella configurazione predefinita del volume, imposta l'efficienza dello storage su Enabled.
14. Lascia le impostazioni rimanenti ai valori predefiniti e scegli Avanti.
15. Esamina gli attributi del file system e scegli Crea file system.

Recupera il nome DNS NFS per la macchina virtuale di archiviazione

1. Vai alla FSx console Amazon.
2. Nel menu a sinistra, seleziona File system.
3. Scegli il file system appena creato.
4. Seleziona la scheda Macchine virtuali di archiviazione.

5. Scegli la macchina virtuale di archiviazione.
6. Seleziona la scheda Endpoints.
7. Copia il nome DNS del file system di rete (NFS) per utilizzarlo successivamente in Vsphere. VMware

Creare un datastore NFS in vSphere utilizzando il volume for ONTAP FSx

Segui le istruzioni in Creare un datastore NFS in un ambiente vSphere per configurare Amazon FSx for NetApp ONTAP come storage esterno per vSphere. VMware Per l'impostazione Server nell'interfaccia client vSphere, utilizzare il nome DNS NFS della macchina virtuale di archiviazione (SVM) copiato nel passaggio precedente.

Configurazione FSx per NetApp ONTAP FSx come datastore iSCSI

La procedura seguente descrive i passaggi minimi necessari FSx per configurare NetApp ONTAP come datastore iSCSI per Amazon EVS utilizzando la console VMware e FSx l'interfaccia client vSphere in esecuzione su Amazon EVS.

Prerequisiti

Prima di utilizzare Amazon EVS con Amazon FSx for NetApp ONTAP, assicurati che le seguenti attività prerequisite siano state completate.

- Un ambiente Amazon EVS viene distribuito nel tuo Virtual Private Cloud (VPC). Per ulteriori informazioni, consulta Nozioni di base.
- Hai accesso al tuo client vSphere in esecuzione su Amazon EVS.
- Tu o il tuo amministratore di storage dovete disporre delle autorizzazioni necessarie per creare e gestire i FSx file system ONTAP nel vostro VPC. Per ulteriori informazioni, consulta Gestione delle identità e degli accessi per Amazon FSx for NetApp ONTAP.

Crea un file system FSx per NetApp ONTAP

1. Vai alla FSx console Amazon.
2. Scegliere Create file system (Crea file system).
3. Seleziona Amazon FSx per NetApp ONTAP.
4. Scegli Next (Successivo).

5. Seleziona Standard create.
6. Per Tipo di implementazione, seleziona un'opzione di implementazione Single-AZ.

> **Note**
>
> Al momento Amazon EVS supporta solo implementazioni Single-AZ.

7. Per la capacità di archiviazione SSD, specificare 1024 GiB.
8. Per Capacità di trasmissione, scegli Specificare la capacità di trasmissione. Scegli almeno 512 MB/s per Single-AZ 1 o almeno 768 MB/s per Single-AZ 2.
9. Seleziona il VPC Amazon EVS con connettività alle sottoreti VLAN Amazon EVS.
10. Seleziona un gruppo di sicurezza che permetta tutto il traffico iSCSI necessario FSx per ONTAP alla sottorete VLAN di gestione dell'host Amazon EVS. VMkernel
11. Seleziona la sottorete di accesso al servizio Amazon EVS in cui verrà distribuito il file system. Per ulteriori informazioni, consulta the section called "Sottorete di accesso al servizio".
12. Nella configurazione predefinita del volume, imposta l'efficienza dello storage su Enabled.
13. Lascia le impostazioni rimanenti ai valori predefiniti e scegli Avanti.
14. Esamina gli attributi del file system e scegli Crea file system.

Configurazione di un adattatore iSCSI software in vSphere for ESX host storage

Per ogni host ESX, è necessario configurare l'adattatore iSCSI software in modo che gli host ESX possano utilizzarlo per accedere allo storage iSCSI. Per istruzioni sulla configurazione dell'adattatore iSCSI software per gli host ESX in vSphere, vedere Aggiungere o rimuovere l'adattatore iSCSI software nella documentazione del prodotto vSphere. VMware

Dopo aver configurato l'adattatore iSCSI software, copiare il nome IQN (iSCSI Qualified Name) associato a un adattatore iSCSI. Questi valori verranno utilizzati in seguito.

Creare un LUN iSCSI

FSx for ONTAP consente di creare numeri di unità logici (LUNs) destinati specificamente all'accesso iSCSI, fornendo storage a blocchi condiviso agli host ESX. Si utilizza l' NetApp ONTAP CLI per creare un LUN.

Di seguito è riportato un comando di esempio.

> **Note**
>
> Si consiglia di configurare la dimensione del LUN al 90% della dimensione del volume.

```
lun create -vserver <your_svm_name> \
-path /vol/<your_volume_name>/<lun_name> \
-size <required_datastore_capacity> \
-ostype vmware
```

Per ulteriori informazioni, vedere Creazione di un LUN iSCSI nella Guida FSx per l'utente di for ONTAP.

Configurare e mappare un gruppo di iniziatori al LUN iSCSI

Dopo aver creato un LUN iSCSI, il passaggio successivo del processo consiste nel creare un gruppo di iniziatori (`igroup`) per connettere il volume al cluster e mappare il LUN al gruppo di iniziatori. Per eseguire queste azioni, si utilizza la CLI di NetApp ONTAP.

1. Configura il gruppo di iniziatori.

   Di seguito è riportato un comando di esempio. Per`--initiator`, utilizzare l'adattatore iSCSI IQNs che è stato copiato nel passaggio precedente.

   ```
   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. Verificare che esista`igroup`.

   ```
   lun igroup show
   ```

3. Mappare il LUN al gruppo di iniziatori. Di seguito è riportato un comando di esempio.

   ```
   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. Utilizzare il `lun show -path` comando per confermare che il LUN è stato creato, online e mappato.

```
lun show -path /vol/<vol_name>/<lun_name> -fields state,mapped,serial-hex
```

Per ulteriori informazioni, vedere Provisioning iSCSI per Linux o Provisioning iSCSI per Windows nella FSx Guida per l'utente di for ONTAP.

Configurare il rilevamento dinamico del LUN iSCSI in vSphere

Per consentire agli host ESX di visualizzare il LUN iSCSI, è necessario configurare il rilevamento dinamico per ogni host nell'interfaccia client vSphere. Per il campo server iSCSI, immettere il nome DNS (NFS) copiato nel passaggio precedente. Per ulteriori informazioni, vedere Configurazione del rilevamento dinamico o statico per iSCSI e iSCSI e iSER su host ESX nella documentazione del prodotto vSphere VMware .

Creare un datastore VMFS in VMware vSphere utilizzando il LUN iSCSI

I datastore Virtual Machine File System (VMFS) fungono da repository per le macchine virtuali. VMware Seguire le istruzioni in Create a vSphere VMFS Datastore per configurare il datastore VMFS in vSphere utilizzando il LUN iSCSI configurato in precedenza. VMware

Risoluzione dei problemi

Questo capitolo descrive alcuni problemi comuni riscontrati durante la creazione o la gestione di ambienti Amazon EVS.

Broadcom e AWS Guida all'assistenza

AWS fornisce supporto per Amazon EVS e i servizi di infrastruttura associati, tra cui VMware Cloud Foundation (VCF). Per indicazioni sulla VCF-specific configurazione o problemi relativi ad altri prodotti VMware come Aria Suite, HCX o NSX, puoi anche contattare Broadcom direttamente utilizzando il tuo diritto all'assistenza Broadcom. Per ulteriori informazioni, consulta Broadcom Support Portal.

Risolvi i problemi relativi ai controlli dello stato dell'ambiente non riusciti

Amazon EVS esegue controlli automatici sul proprio ambiente per identificare i problemi. È possibile visualizzare lo stato dell'ambiente per identificare problemi specifici e rilevabili.

Rivedi le informazioni sul controllo dello stato dell'ambiente

Per analizzare gli ambienti compromessi utilizzando la console Amazon EVS

1. Apri la console Amazon EVS.
2. Nel pannello di navigazione, scegli Ambienti, quindi seleziona il tuo ambiente.
3. Seleziona la scheda Dettagli per visualizzare una panoramica dell'ambiente.
4. Controlla lo stato dell'ambiente. Passa il mouse su questo campo per espandere un popover con i risultati individuali per ogni controllo dello stato dell'ambiente.

Controllo di raggiungibilità non riuscito

Il controllo di raggiungibilità verifica che Amazon EVS disponga di una connessione persistente a SDDC Manager. Se Amazon EVS non riesce a raggiungere l'ambiente, questo controllo ha esito negativo.

In tal caso, Amazon EVS non può più contattare SDDC Manager per convalidare lo stato dell'ambiente e gli host non possono più essere aggiunti all'ambiente. La mancata raggiungibilità causerà inoltre il fallimento del riutilizzo della chiave di licenza e dei controlli di copertura delle chiavi e il controllo del conteggio degli host restituirà una risposta Sconosciuto.

Per garantire la raggiungibilità, verifica quanto segue:

- Assicurati che i certificati siano validi e non scaduti. È possibile utilizzare l'interfaccia utente di SDDC Manager o il client vSphere per gestire i certificati in un ambiente VCF. Dopo l'implementazione, si consiglia di sostituire tutti i certificati del dominio di gestione di VMware Cloud Foundation. Per ulteriori informazioni, vedere Gestione dei certificati in VMware Cloud Foundation nella documentazione di VMware Cloud Foundation.
- Assicurati che i tuoi server DNS siano raggiungibili dalla sottorete di accesso al servizio, che i record DNS siano validi e che non esistano nomi host o indirizzi IP duplicati.
- Per creare le regole del firewall, segui queste linee guida:
  - Consenti l'accesso ai server TCP/UDP DNS.
  - Consenti HTTPS/SSH l'accesso alla sottorete VLAN di gestione dell'host.
  - Consenti HTTPS/SSH l'accesso alla sottorete VLAN di Management VM.

Se non riesci ancora a risolvere il problema dopo aver seguito questa guida, ti consigliamo di contattare il AWS servizio Support per ulteriore assistenza.

Controllo del conteggio degli host non riuscito

Questo controllo verifica che l'ambiente disponga di un minimo di quattro host, requisito per VCF 5.2.x.

Se questo controllo ha esito negativo, sarà necessario aggiungere host in modo che il proprio ambiente soddisfi questo requisito minimo. Amazon EVS supporta solo ambienti con 4-32 host.

Controllo del riutilizzo delle chiavi non riuscito

Questo controllo verifica che la chiave di licenza VCF non sia utilizzata da un altro ambiente Amazon EVS. Le licenze VCF possono essere utilizzate per un solo ambiente Amazon EVS. Questo controllo non riesce se fornisci chiavi di licenza VCF in una richiesta di creazione di ambiente che sono già utilizzate da un altro ambiente.

In tal caso, si riceverà una risposta di errore che indica che non è stato possibile creare l'ambiente Amazon EVS. Per risolvere il problema, controlla le impostazioni delle licenze in SDDC Manager e sostituisci le licenze utilizzate in precedenza con licenze inutilizzate.

> **Important**
>
> Utilizza l'interfaccia utente SDDC Manager per gestire la soluzione VCF e le chiavi di licenza vSAN. Amazon EVS richiede il mantenimento di una soluzione VCF valida e delle chiavi di licenza vSAN in SDDC Manager per il corretto funzionamento del servizio. Sebbene le chiavi debbano essere assegnate agli host e al cluster vSAN utilizzando vSphere Client, è necessario assicurarsi che tali chiavi vengano visualizzate anche nella schermata delle licenze dell'interfaccia utente di SDDC Manager.

Controllo della copertura delle chiavi non riuscito

Questo controllo verifica che la chiave di licenza VCF assegnata a vCenter Server allochi core vCPU e capacità di archiviazione vSAN (TiB) sufficienti per tutti gli host implementati.

In tal caso, si riceverà una risposta di errore che indica che non è stato possibile creare l'ambiente Amazon EVS. La mancata copertura della chiave può indicare uno dei seguenti problemi:

- Le licenze VCF non sono assegnate correttamente a vCenter Server. È necessario assegnare una licenza a vCenter Server prima della scadenza del periodo di valutazione o della licenza attualmente assegnata. Se questo è il problema, rivedi le assegnazioni delle licenze in SDDC Manager.
- Le attuali licenze VCF non coprono le esigenze di capacità di storage vCPU core e vSAN. I requisiti per la chiave della soluzione VCF (incluso il numero minimo di core) e la chiave di licenza vSAN (inclusa la capacità minima di vSAN) variano a seconda del tipo di istanza. Per le soglie specifiche per la configurazione, consulta. the section called "Abbonamenti VCF" Se questo è il problema, aggiungi le licenze vSAN in SDDC Manager fino a soddisfare le tue esigenze di utilizzo.

Se le azioni precedenti non risolvono il problema, contatta il AWS Supporto per ulteriore assistenza.

> **Important**
>
> Utilizza l'interfaccia utente SDDC Manager per gestire la soluzione VCF e le chiavi di licenza vSAN. Amazon EVS richiede il mantenimento di una soluzione VCF valida e delle chiavi

di licenza vSAN in SDDC Manager per il corretto funzionamento del servizio. Sebbene le chiavi debbano essere assegnate agli host e al cluster vSAN utilizzando vSphere Client, è necessario assicurarsi che tali chiavi vengano visualizzate anche nella schermata delle licenze dell'interfaccia utente di SDDC Manager.

L'agente vSphere HA su questo host non è riuscito a raggiungere l'indirizzo di isolamento

<IPv6 address>Nell'interfaccia utente vCenter, con l'host ESX selezionato, viene visualizzato il messaggio «vSphere HA agent on this host could not reach isolation address».

Questo messaggio di errore indica che l'agente vSphere HA su un host non è in grado di raggiungere l'indirizzo di isolamento IPv6 predefinito utilizzato da vSphere HA per i controlli del battito cardiaco. Il messaggio di errore non è indicativo di un problema e si verifica solo perché Amazon EVS non supporta IPv6 in questo momento. L'assenza del supporto IPV6 per Amazon EVS non influisce sulle funzionalità di base di vSphere HA.

I precontrolli di aggiornamento di vSAN non riescono per il cluster host ESX

Quando si tenta di aggiornare il cluster host ESX utilizzando SDDC Manager, i precontrolli relativi al disco vSAN potrebbero non riuscire. Questo perché Amazon EVS utilizza vSAN Express Storage Architecture (ESA) e i precontrolli di aggiornamento non si applicano a vSAN ESA. Per ulteriori informazioni, consulta l'articolo della knowledge base di Broadcom su questo argomento.

Errore di aggiunta dell'host dovuto a un'immagine del cluster incompatibile

Problema

Quando aggiungi un host al tuo ambiente, l'host dispone dell'ultima versione disponibile del componente aggiuntivo personalizzato EVS del fornitore. Se il tuo ambiente utilizza host con una versione del componente aggiuntivo precedente, l'aggiunta di nuovi host non riesce e viene visualizzato un errore che indica che il nuovo host non è compatibile con l'immagine del cluster. Per

risolvere questo problema, è necessario utilizzare vSphere Lifecyle Manager per estrarre l'ultima versione aggiuntiva disponibile dall'host appena aggiunto.

Soluzione

Segui questa procedura.

1. Vai all'inventario degli host e dei cluster in VMware vCenter Server.
2. Estrai il componente aggiuntivo dall'host appena aggiunto creando un cluster vuoto temporaneo.
3. In Nozioni di base, selezionare Importa immagine da un host esistente nel vCenter Inventory e creare il cluster. Lascia tutte le altre impostazioni come predefinite.
4. Una volta creato questo cluster temporaneo con l'immagine estratta, è possibile eliminare il cluster temporaneo. Il componente aggiuntivo sarà ora disponibile nel depot di vSphere Lifecycle Manager.
5. Vai al cluster dell'ambiente e seleziona la scheda Aggiornamenti.
6. Modifica l'immagine del cluster e cambia la versione del componente aggiuntivo con la versione appena estratta.
7. Scegli Save (Salva).
8. In SDDC Manager, riprova l'operazione di aggiunta host non riuscita. Questa operazione correggerà gli host del cluster, aggiornando tutti gli host alla versione aggiuntiva più recente. La riparazione delle immagini del cluster richiederà il riavvio dell'host.

SDDC Manager non riesce a convalidare l'host VCF durante la messa in servizio dell'host

Problema

Se hai aggiornato la tua versione ESX dopo l'implementazione dell'ambiente Amazon EVS, SDDC Manager potrebbe fallire durante la convalida dell'host VCF nella fase di commissione degli host. Per risolvere questo problema, sarà necessario utilizzare vSphere Lifecyle Manager per aggiornare ESX sull'host appena aggiunto.

Soluzione

Segui questa procedura.

> **Important**
>
> Questi passaggi richiedono l'aggiunta temporanea dell'host a vCenter al di fuori di SDDC Manager. L'utilizzo di vSphere Lifecyle Manager per qualsiasi operazione diversa dagli upgrade ESX può rendere l'host inutilizzabile e richiedere l'eliminazione e la creazione di un nuovo host Amazon EVS.

1. Vai all'inventario degli host e dei cluster in VMware vCenter Server.
2. Aggiungi temporaneamente l'host al tuo data center virtuale, assicurandoti di selezionare Gestisci host con un'immagine. L'host verrà rimosso in una fase successiva dopo il completamento dell'aggiornamento ESX. Per ulteriori informazioni, vedere Come aggiungere un host al data center o alla cartella vSphere nella documentazione di vSphere.
3. Una volta aggiunto l'host a vSphere, aggiornare la versione ESX sull'host. Questa operazione può essere eseguita nella scheda Aggiornamenti dell'host. Modifica l'immagine dell'host in modo che corrisponda alla versione ESX del cluster.
4. Una volta completato l'aggiornamento, rimuovi l'host dal tuo inventario vCenter. Per ulteriori informazioni, vedere Come rimuovere un host ESX dall'istanza di vCenter Server nella documentazione di vSphere.
5. Metti in servizio il tuo host in SDDC Manager. Per ulteriori informazioni, consulta Commission Hosts nella documentazione di VMware Cloud Foundation.
6. Dopo la messa in servizio dell'host, aggiungi l'host al cluster utilizzando SDDC Manager.

Lo stato di autorizzazione di Windows Server è A rischio a causa di un errore di raggiungibilità dell'appliance

Un'autorizzazione entra in uno stato di rischio quando il connettore Amazon EVS associato non supera il controllo di raggiungibilità per l'appliance di gestione VCF. Per le autorizzazioni Windows Server, hai a disposizione 8 ore dal momento in cui l'autorizzazione raggiunge lo stato di rischio per ripristinare la connessione. Se la connessione non viene ripristinata entro questo periodo, le autorizzazioni vengono automaticamente eliminate e il monitoraggio dell'utilizzo di Windows Server viene interrotto.

Per risolvere questo problema, controlla quanto segue:

- Verifica che lo stato del connettore sia Attivo e che il relativo controllo di raggiungibilità sia Non riuscito.
- Verificare che le credenziali dell'appliance memorizzate in AWS Secrets Manager siano aggiornate e corrette. Se le credenziali sono state ruotate nell'appliance, aggiorna i valori nel segreto esistente di Secrets Manager. Se è necessario indicare un segreto diverso, utilizzare per UpdateEnvironmentConnector aggiornare l'identificatore segreto.
- Assicurati che i server DNS siano raggiungibili dalla sottorete di accesso al servizio, che i record DNS per l'FQDN dell'appliance siano validi e che non esistano nomi host o indirizzi IP duplicati.
- Verifica che le regole del firewall consentano l'accesso alla sottorete VLAN della macchina virtuale di gestione e l' HTTPS/SSH accesso ai server DNS. TCP/UDP
- Assicurati che l'appliance sia funzionante e accessibile.

Una volta ripristinata la connessione, le autorizzazioni torneranno automaticamente allo stato corretto di Creato. Se le autorizzazioni sono già state eliminate e hanno lo stato Entitlement Removed, è necessario creare nuove autorizzazioni dopo che il connettore è tornato allo stato Attivo con un controllo di raggiungibilità superato.

Se non riesci ancora a risolvere il problema dopo aver seguito questa guida, ti consigliamo di contattare il AWS servizio Support per ulteriore assistenza.

L'autorizzazione non è riuscita a causa di un sistema operativo guest non supportato

La creazione di un'autorizzazione non riesce o un'autorizzazione esistente viene rimossa quando Amazon EVS rileva che sulla macchina virtuale è in esecuzione un sistema operativo guest non supportato per Amazon EVS Windows Server Licensing.

Ciò può verificarsi quando:

- Una macchina virtuale con un'autorizzazione Windows Server esistente viene riconfigurata per utilizzare una versione del sistema operativo non supportata o un sistema operativo non Windows.
- La creazione di un'autorizzazione non è riuscita a causa di una macchina virtuale che esegue già un sistema operativo guest non supportato.

Per risolvere il problema:

- Verifica che lo stato del connettore sia Attivo e che il relativo stato di controllo della raggiungibilità sia stato superato.
- Verifica il sistema operativo guest configurato sulla macchina virtuale. Amazon EVS Windows Server Licensing supporta Windows Server 2016 o versioni successive.
- Riconfigura la macchina virtuale per utilizzare una versione di Windows Server supportata.
- Dopo aver aggiornato il sistema operativo guest, crea una nuova autorizzazione per la macchina virtuale.
- (Facoltativo) Eliminare l'autorizzazione nello stato Entitlement Removed.

Se non riesci ancora a risolvere il problema dopo aver seguito questa guida, ti consigliamo di contattare il AWS servizio Support per ulteriore assistenza.

Lo stato di diritto è stato rimosso

Un'autorizzazione con lo stato Entitlement Removed indica che Amazon EVS ha rimosso l'autorizzazione per la macchina virtuale. Quando viene rimossa un'autorizzazione, il monitoraggio dell'utilizzo di Windows Server si interrompe per la macchina virtuale interessata.

Questo stato può derivare da diverse cause:

- Errore di raggiungibilità dell'apparecchiatura che ha superato il periodo di prova di 8 ore. Per informazioni, consulta the section called "Lo stato di autorizzazione di Windows Server è A rischio a causa di un errore di raggiungibilità dell'appliance".
- La VM non è più presente nell'inventario dell'appliance. Per informazioni, consulta the section called "Autorizzazione rimossa a causa della disconnessione, dell'isolamento o della mancanza della macchina virtuale dall'inventario".
- La VM è stata disconnessa o isolata dal suo host. Per informazioni, consulta the section called "Autorizzazione rimossa a causa della disconnessione, dell'isolamento o della mancanza della macchina virtuale dall'inventario".
- Il sistema operativo guest VM è stato modificato in una versione non supportata. Per informazioni, consulta the section called "L'autorizzazione non è riuscita a causa di un sistema operativo guest non supportato".

Per ripristinare l'autorizzazione:

- Controlla i dettagli dell'errore dell'autorizzazione per identificare la causa specifica della rimozione.

- Risolvi il problema di fondo.
- Crea una nuova autorizzazione per la macchina virtuale una volta che il connettore è in uno stato Attivo con un controllo di raggiungibilità in uno stato Passed.
- (Facoltativo) Eliminare l'autorizzazione nello stato Entitlement Removed.

Se non riesci ancora a risolvere il problema dopo aver seguito questa guida, ti consigliamo di contattare il AWS servizio Support per ulteriore assistenza.

Autorizzazione rimossa a causa della disconnessione, dell'isolamento o della mancanza della macchina virtuale dall'inventario

Un'autorizzazione viene rimossa quando Amazon EVS rileva che una macchina virtuale è stata disconnessa, isolata o non è più presente nell'inventario dell'appliance. L'autorizzazione viene rimossa immediatamente e il tracciamento dell'utilizzo viene interrotto.

Per risolvere il problema:

- Verifica che lo stato del connettore sia Attivo e che lo stato del controllo di raggiungibilità sia stato superato.
- Controlla lo stato della connessione della macchina virtuale nel tuo dispositivo. Una macchina virtuale disconnessa o isolata può indicare un problema sull'host o sulla rete.
- Risolve il problema dell'host o della rete sottostante che causa la disconnessione o l'isolamento della macchina virtuale.
- Dopo che la macchina virtuale è stata ricollegata e ha funzionato normalmente, crea una nuova autorizzazione per riprendere l'utilizzo di Windows Server.

Se non riesci ancora a risolvere il problema dopo aver seguito questa guida, ti consigliamo di contattare il AWS servizio Support per ulteriore assistenza.

Registrazione delle chiamate API Amazon EVS tramite AWS CloudTrail

Amazon EVS è integrato con AWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente IAM, da un ruolo IAM o da un AWS servizio in Amazon EVS. CloudTrail acquisisce tutte le chiamate AWS API per Amazon EVS come eventi. Le chiamate acquisite includono chiamate dalla console Amazon EVS e chiamate in codice alle operazioni dell'API Amazon EVS. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per Amazon EVS. Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare la richiesta che è stata effettuata ad Amazon EVS, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Per ulteriori informazioni CloudTrail, consulta la Guida per l'AWS CloudTrail utente.

> **Note**
>
> Amazon EVS non registra le attività degli utenti per elementi non AWS componenti, ad esempio le attività all'interno dell'ambiente VCF. Queste attività vengono registrate in varie VMware console come vSphere e NSX Manager.
> Se si desidera una registrazione VCF centralizzata, è possibile configurare soluzioni di monitoraggio VCF come VMware Cloud Foundation Operations per ottenere questo risultato.

Informazioni su Amazon EVS in CloudTrail

CloudTrail è abilitato sul tuo AWS account al momento della creazione dell'account. Quando si verifica un'attività in Amazon EVS, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi di AWS servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare eventi recenti nel tuo AWS account. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi nel tuo AWS account, inclusi gli eventi per Amazon EVS, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando crei un percorso nella console, il percorso si applica a tutte le

AWS regioni. Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- CloudTrail servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni
- Ricezione di file di CloudTrail registro da più account

Tutte le azioni di Amazon EVS vengono registrate CloudTrail e documentate nell'Amazon EVS API Reference. Ad esempio, le chiamate a `GetEnvironment` e le `CreateEnvironment` `DeleteEnvironment` azioni generano voci nei file di registro. CloudTrail

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Comprendere le voci dei file di registro di Amazon EVS

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

Quote di servizio Amazon EVS

Amazon EVS è integrato con Service Quotas e puoi utilizzarlo per visualizzare e gestire le tue quote da Servizio AWS una posizione centrale. Per ulteriori informazioni, consulta Cos'è Service Quotas? nella Guida per l'utente di Service Quotas.

Con l'integrazione di Service Quotas, puoi utilizzare Console di gestione AWS o AWS CLI per cercare il valore delle tue quote Amazon EVS e richiedere un aumento delle quote per le quote regolabili. Per ulteriori informazioni, vedere Richiesta di aumento della quota nella Service Quotas User Guide request-service-quota-increasee nel AWS CLI Command Reference.

Per ulteriori informazioni sulle quote dei servizi Amazon EVS, consulta le quote Amazon EVS nella Guida di riferimento generale. AWS

Important

Assicurati che la quota di istanze EC2 Running On-Demand Standard rifletta il numero di vCPU necessarie per tutte le istanze EC2 che utilizzerai su Amazon EVS. Per informazioni sull'aumento delle quote di servizio EC2, consulta Request an increase in Amazon EC2 User Guide.

Note

Se prevedi di utilizzare gli host dedicati EC2 per il tuo ambiente Amazon EVS, assicurati che la quota di host dedicati EC2 rifletta il numero di host dedicati che intendi utilizzare per una regione desiderata. Per informazioni sull'aumento delle quote di servizio EC2, consulta Request an increase in Amazon EC2 User Guide.

Note

Se configuri la connettività Internet HCX, la tua quota IPAM per la lunghezza della netmask a blocchi IPv4 CIDR pubblici contigui fornita da Amazon deve essere /28 o superiore. Per ulteriori informazioni, consulta Quote per il tuo IPAM.

> **Note**
>
> Amazon CloudWatch raccoglie i parametri di AWS utilizzo per le risorse Amazon EVS con quote (ambiente e host). Per ulteriori informazioni, consulta CloudWatch Usage Metrics nella Amazon CloudWatch User Guide.

Visualizza le quote dei servizi Amazon EVS nel Console di gestione AWS

1. Apri la console Service Quotas.
2. Nel riquadro di navigazione a sinistra, scegli AWS servizi.
3. Dall'elenco dei AWS servizi, cerca e seleziona Amazon Elastic VMware Service.
4. Scegli Visualizza quote.

   Nell'elenco delle quote di servizio, puoi vedere il nome della quota di servizio, il valore applicato (se disponibile), la quota AWS predefinita e se il valore della quota è regolabile.
5. Per visualizzare ulteriori informazioni su una quota di servizio, ad esempio la descrizione, scegli il nome della quota.
6. (Facoltativo) Per richiedere un aumento della quota, seleziona la quota che desideri aumentare, seleziona Richiedi aumento a livello di account, inserisci o seleziona le informazioni richieste e seleziona Richiedi.

Per utilizzare meglio le quote di servizio utilizzando la Console di gestione AWS, consulta la Service Quotas User Guide. Per richiedere un aumento delle quote, consultare Richiesta di aumento delle quote nella Guida per l'utente di Service Quotas.

Visualizza le quote dei servizi Amazon EVS con la CLI AWS

Esegui il comando seguente per visualizzare le tue quote Amazon EVS.

```
aws service-quotas list-aws-default-service-quotas \
    --query 'Quotas[*].
{Adjustable:Adjustable,Name:QuotaName,Value:Value,Code:QuotaCode}' \
    --service-code evs \
```

```
    --output table
```

> **Note**
>
> La quota restituita è il numero di ambienti o host Amazon EVS che possono essere creati in questo account nella AWS regione corrente.

Per lavorare di più con le quote di servizio utilizzando la AWS CLI, consulta service-quotas nel AWS CLI Command Reference. Per richiedere un aumento della quota, consulta il request-service-quota-increasecomando nella AWS CLI Command Reference.

Cronologia dei documenti per la Amazon Elastic VMware Service User Guide

La tabella seguente descrive le versioni della documentazione per Amazon Elastic VMware Service.

Modifica	Descrizione	Data
Aggiunto l'argomento Amazon EVS Custom Addon depot	È stata aggiunta la documentazione per accedere al depot Amazon EVS Custom Addon. Puoi utilizzare l'azione `GetDepotUrl` API per recuperare un URL di depot e configurarlo come sorgente di download in vSphere Lifecycle Manager (vLCM) per sincronizzare e installare l'Amazon EVS Custom Addon.	21 maggio 2026
È stato aggiunto il supporto per 32 host per ambiente EVS	Amazon EVS ora supporta fino a 32 host per ambiente EVS.	18 maggio 2026
È stato aggiunto il supporto per il tipo di istanza	Amazon EVS ora supporta il tipo di istanza i7i.metal-24xl da utilizzare con ambienti EVS. Questo tipo di istanza bare-metal è disponibile in tutte le versioni di VMware Cloud Foundation (VCF).	27 aprile 2026
Aggiunti i connettori ambientali e le guide per gli utenti con autorizzazione	Sono state aggiunte guide utente per la gestione dei connettori e delle autorizzazioni dell'ambiente Amazon EVS. I connettori stabiliscono una connessione persistente	20 aprile 2026

	tra Amazon EVS e un'applia nce VCF, abilitando funzional ità come Windows License Included. Le autorizzazioni ti consentono di abilitare o rimuovere la copertura delle licenze di Windows Server per le macchine virtuali nel tuo ambiente Amazon EVS.	
Aggiornato AmazonEVS ServiceRolePolicy	Amazon EVS ha aggiornato la policy gestita `AmazonEVS ServiceRolePolicy` per consentire al servizio di recuperare le credenzia li vCenter da Secrets AWS Manager e di decrittografare i segreti crittografati con chiavi KMS gestite dal cliente.	23 marzo 2026
Supporto al rilascio per VCF-5.2.2	Amazon EVS ora supporta la VCF-5.2.2 possibilità di specificare combinazioni supportate di versioni software VMware Cloud Foundatio n (VCF) ed ESX durante la configurazione degli ambienti e degli host EVS.	20 gennaio 2026

Amazon EVS rilasciato in più regioni AWS	Amazon EVS è stato rilasciato nelle regioni Stati Uniti occidentali (California settentrionale), Asia Pacifico (Hyderabad), Asia Pacifico (Malesia), Canada occidentale (Calgary), Europa (Milano), Messico (Centrale) e Sud America (San Paolo).	15 dicembre 2025
Amazon EVS rilasciato in più regioni AWS	Amazon EVS è stato rilasciato nelle regioni Asia Pacifico (Mumbai), Asia Pacifico (Sydney), Canada (Centrale) ed Europa (Parigi).	6 novembre 2025
Amazon EVS è stato rilasciato nelle regioni Asia Pacifico (Singapore) ed Europa (Londra)	Amazon EVS è stato rilasciato nelle regioni Asia Pacifico (Singapore) ed Europa (Londra).	30 settembre 2025
Amazon EVS supporta la migrazione HCX su Internet pubblico	Amazon EVS ora ti consente di migrare ed estendere in modo sicuro le tue reti di livello 2 dai data center locali agli ambienti Amazon EVS tramite la rete Internet pubblica.	18 settembre 2025

Aggiornato AmazonEVS ServiceRolePolicy	Amazon EVS ha aggiornato la policy gestita `AmazonEVS ServiceRolePolicy` per aggiungere funzionalità complete di gestione delle risorse, tra cui la gestione delle istanze EC2, le operazioni sui volumi EBS e l'integrazione di AWS Secrets Manager. Per informazioni, consulta gli aggiornamenti di Amazon EVS alle policy AWS gestite.	14 agosto 2025
Aggiornato AmazonEVS ServiceRolePolicy	È stata aggiornata la politica AWS AmazonEVSServiceRolePolicy gestita.	4 agosto 2025
È stato rilasciato il conteggio dell'ambiente per quota di AWS account	Numero di ambienti rilasciati da Amazon EVS per quota di AWS account. Il numero di ambienti per quota di AWS account rappresenta il numero massimo di ambienti Amazon EVS che è possibile creare in un determinato account e regione.	8 luglio 2025
Amazon EVS rilasciato nella regione Europa (Irlanda)	Amazon EVS è stato rilasciato nella regione Europa (Irlanda).	18 giugno 2025
Rilasciato AmazonEVS ServiceRolePolicy	La politica AWS gestita AmazonEVSServiceRolePolicy è stata rilasciata.	9 giugno 2025

Versione iniziale della Guida per l'utente	È stata rilasciata la Amazon Elastic VMware Service User Guide. La Amazon EVS User Guide descrive tutti i concetti di Amazon EVS e fornisce istruzioni sull'uso delle varie funzionalità sia con la console che con l'interfaccia a riga di comando.	9 giugno 2025

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.