Guide de l’utilisateur

# Amazon Elastic VMware Service

# Amazon Elastic VMware Service: Guide de l’utilisateur

# Table of Contents

# Qu'est-ce qu'Amazon Elastic VMware Service ?

Vous pouvez utiliser Amazon Elastic VMware Service (Amazon EVS) pour déployer et exécuter un environnement VMware Cloud Foundation (VCF) directement sur des instances EC2 bare metal au sein de ( Amazon Virtual Private Cloud VPC).

Rubriques



## Caractéristiques d'Amazon EVS

Les principales fonctionnalités d'Amazon EVS sont les suivantes :

Simplifiez et accélérez votre migration vers AWS

> Éliminez les frictions liées à la migration et garantissez la cohérence opérationnelle grâce à la portabilité des abonnements et au déploiement automatisé de VMware Cloud Foundation (VCF) dans le cloud. Étendez les réseaux sur site et migrez les charges de travail sans avoir à modifier les adresses IP, à recycler le personnel ou à réécrire les runbooks opérationnels.

Gardez le contrôle de votre VMware architecture dans le cloud

> Gardez le contrôle total de votre VMware architecture et optimisez une pile de virtualisation qui répond aux exigences uniques de vos applications, y compris les modules complémentaires et les solutions tierces.

Gérez vous-même ou tirez parti AWS des partenaires pour une expérience gérée

> Profitez du choix et de la flexibilité nécessaires à l'autogestion, ou tirez parti de l'expertise des AWS partenaires pour gérer et exploiter votre environnement VCF AWS afin d'atteindre vos objectifs commerciaux en termes de talents, de temps et de coûts.

Développez et protégez votre entreprise contre les perturbations

Améliorez l'évolutivité sur le cloud le plus sécurisé, évolutif et résilient pour la migration et l'exploitation de vos charges de travail VMware basées sur le cloud.

Optez pour AWS l'innovation pour transformer vos applications et votre infrastructure

En tant que service AWS natif, Amazon EVS simplifie l'extension et l'extension de votre VMware environnement grâce à plus de 200 services (notamment des bases de données gérées, des outils d'analyse, des solutions sans serveur et des conteneurs, ainsi que l'IA générative) destinés à transformer votre entreprise.

# Commencez à utiliser Amazon EVS

Pour créer votre premier environnement Amazon EVS, consultezPrise en main. En général, pour démarrer avec Amazon EVS, vous devez suivre les étapes suivantes.

1. Prérequis pour Pour de plus amples informations, veuillez consulter Configuration d'Amazon Elastic VMware Service.
2. Créez un environnement Amazon EVS. Lors de la création de l'environnement, Amazon EVS crée les sous-réseaux VLAN requis à l'aide des plages CIDR que vous spécifiez et ajoute des hôtes à l'environnement.
3. Personnalisez VCF. Configurez votre environnement dans l'interface utilisateur de vSphere en fonction de vos besoins. Cela peut inclure la configuration des connexions, des politiques, de la surveillance, etc.
4. Connectez-vous et migrez. Connectez votre environnement à votre centre de données sur site et migrez vos charges de travail VCF vers Amazon EVS.

# Accès à Amazon EVS

Vous pouvez définir et configurer vos déploiements Amazon EVS à l'aide des interfaces suivantes :

- Console Amazon EVS : fournit une interface Web pour créer des environnements Amazon EVS.
- AWS CLI - Fournit des commandes pour un large éventail de systèmes Services AWS et est compatible avec Windows, macOS et Linux. Pour de plus amples informations, veuillez consulter AWS Command Line Interface.

- AWS CloudFormation - Fournit une spécification pour chaque type de ressource, par exemple`AWS::EVS::Environment`. Vous créez un modèle à l'aide de la spécification des ressources et vous vous CloudFormation occupez de l'approvisionnement et de la configuration des ressources pour vous.

# Concepts et composants d'Amazon EVS

Cette section explique certains concepts et composants clés d'Amazon EVS.

## Environnement Amazon EVS

Un environnement Amazon EVS est un conteneur logique pour les ressources VMware Cloud Foundation (VCF), telles que les hôtes vSphere, vSAN, NSX et SDDC Manager. Un environnement contient un domaine VCF consolidé avec un cluster vSphere qui héberge les composants de gestion, de surveillance et d'instanciation de la pile logicielle VCF. Chaque environnement est directement mappé à une appliance SDDC Manager. Pour de plus amples informations, veuillez consulter the section called "Architecture".

## Hôte Amazon EVS

Un hôte Amazon EVS est un hôte VMware ESX qui s'exécute sur des instances Amazon EC2 bare metal. Les hôtes Amazon EVS utilisent des volumes de stockage d' NVMe instance locaux pour les banques de données vSAN, qui stockent vos machines virtuelles de gestion et de charge de travail.

> **Warning**
>
> Les volumes de stockage d'instances sont éphémères. Les données stockées sur ces volumes ne sont pas conservées si l'instance EC2 sous-jacente est arrêtée ou arrêtée. L'arrêt ou la résiliation d' Amazon EC2 instances utilisées par Amazon EVS sans mise hors service au sein de VCF peut entraîner une perte de données.
> Pour plus d'informations sur la maintenance de l'hôte, consultezthe section called "Maintenance de l'hôte".

## Sous-réseau d'accès au service

Le sous-réseau d'accès au service est un sous-réseau VPC standard qui permet à Amazon EVS d'accéder au déploiement VCF. Lors de la création de l'environnement Amazon EVS, vous spécifiez le VPC et le sous-réseau qu'Amazon EVS doit utiliser pour l'accès au service.

Lorsque vous créez un environnement Amazon EVS, Amazon EVS fournit des interfaces réseau élastiques dans le sous-réseau d'accès aux services afin de faciliter la connectivité de gestion aux appliances VCF et aux hôtes ESX. Cette connectivité est requise pour qu'Amazon EVS puisse déployer, gérer et surveiller le déploiement du VCF.

## Sous-réseau VLAN Amazon EVS

Un sous-réseau Amazon EVS VLAN est un sous-réseau Amazon VPC géré par Amazon EVS. Les sous-réseaux VLAN fournissent une connectivité VPC aux hôtes Amazon EVS et aux dispositifs VCF tels que NSX, VMware HCX et vCenter Server. VMware VMware Chaque sous-réseau VLAN possède une balise VLAN qui permet de segmenter le trafic réseau VLAN de manière logique.

Amazon EVS crée tous les sous-réseaux VLAN utilisés par le service lors de la création de l'environnement Amazon EVS. Vous fournissez les entrées de bloc CIDR utilisées par les sous-réseaux VLAN. Vous devez vous assurer que les blocs CIDR de votre sous-réseau VLAN sont correctement dimensionnés en fonction du nombre d'hôtes qui seront configurés, en tenant compte des futurs besoins de dimensionnement. Les blocs CIDR doivent avoir une taille minimale de masque réseau /28 et une taille maximale de masque réseau /24. Les blocs d'adresse CIDR ne doivent pas se chevaucher avec un bloc d'adresse CIDR existant associé au VPC.

Lors de leur création, les sous-réseaux VLAN sont implicitement associés à la table de routage principale de votre VPC. Après le déploiement, vous pouvez associer explicitement des sous-réseaux VLAN à une table de routage personnalisée. Pour de plus amples informations, veuillez consulter the section called “Considérations relatives au réseau Amazon EVS”.

> **Important**
>
> Les sous-réseaux VLAN Amazon EVS ne peuvent être créés que lors de la création de l'environnement Amazon EVS et ne peuvent pas être modifiés une fois l'environnement créé. Vous devez vous assurer que les blocs CIDR du sous-réseau VLAN sont correctement dimensionnés avant de créer l'environnement. Vous ne pourrez pas ajouter de sous-réseaux VLAN une fois l'environnement déployé.

> **Important**
>
> Les règles du groupe de sécurité EC2 ne sont pas appliquées sur les interfaces réseau élastiques Amazon EVS connectées à des sous-réseaux VLAN. Pour contrôler le trafic à destination et en provenance des sous-réseaux VLAN, vous devez utiliser une liste de contrôle d'accès réseau.

## Sous-réseau VLAN de gestion de l'hôte

Le sous-réseau VLAN de gestion des hôtes sépare le trafic de gestion du trafic utilisateur et permet la gestion à distance des hôtes. L'interface réseau vmkernel de gestion des hôtes EVS se connecte à ce sous-réseau.

## Sous-réseau VLAN vMotion

Le sous-réseau VLAN vMotion segmente logiquement le trafic vMotion et est utilisé au cours d'un processus VMware vMotion pour déplacer des machines virtuelles entre des hôtes.

## Sous-réseau VLAN vSAN

Le sous-réseau VLAN vSAN est utilisé par vSAN pour séparer le trafic lié aux VMware opérations de stockage de vSAN du reste du trafic réseau.

## Sous-réseau VLAN VTEP

Le sous-réseau VLAN VTEP utilise les points de terminaison du tunnel virtuel (VTEP) VMware NSX pour encapsuler et décapsuler le trafic réseau superposé pour les hôtes Amazon EVS ESX.

## Sous-réseau VLAN VTEP Edge

Le sous-réseau VLAN VTEP Edge est un sous-réseau VLAN VTEP spécialisé dédié au trafic de superposition du dispositif NSX Edge. Ce VLAN est utilisé pour les communications par superposition entre NSX Edge et les hôtes ESX.

## Sous-réseau VLAN de la machine virtuelle de gestion

Le sous-réseau VLAN de la machine virtuelle de gestion est utilisé pour gérer les dispositifs virtuels, notamment NSX Manager, vCenter Server et SDDC Manager.

### Sous-réseau VLAN à liaison montante HCX

Le sous-réseau VLAN à liaison montante HCX est utilisé pour la communication entre les appareils HCX Interconnect (HCX-IX) et HCX Network Extension (HCX-NE), et permet la création de la liaison montante du maillage du service HCX.

### Sous-réseau VLAN NSX Uplink

Le sous-réseau VLAN NSX Uplink est utilisé pour connecter vos réseaux de superposition NSX au reste de votre VPC et à tout autre réseau externe que vous configurez. Le sous-réseau VLAN NSX Uplink est configuré sur les liaisons montantes du nœud NSX Edge.

### Sous-réseau VLAN d'extension

Le sous-réseau VLAN d'extension peut être utilisé pour activer des fonctions supplémentaires prises en charge par le VCF, telles que NSX Federation. Amazon EVS crée deux sous-réseaux VLAN d'extension lors de la création de l'environnement.

## VMware NSX

VMware NSX est une plate-forme réseau définie par logiciel (SDN) qui permet la virtualisation du réseau. Amazon EVS utilise VMware NSX pour créer et gérer le réseau superposé sur lequel s'exécutent les appliances et les charges de travail VMware Cloud Foundation (VCF). Amazon EVS déploie une paire de nœuds Active/Standby NSX Edge, ainsi qu'un réseau de superposition NSX. Amazon EVS configure automatiquement l'ensemble du routage et des liaisons montantes NSX en votre nom dans le cadre du déploiement. Pour plus d'informations sur les concepts courants de NSX, consultez la section Concepts clés du guide d'installation de VMware NSX.

## VMware Extension de cloud hybride (HCX)

VMware Hybrid Cloud Extension (VMware HCX) est une plateforme de mobilité des applications conçue pour simplifier la migration des applications, rééquilibrer les charges de travail et optimiser la reprise après sinistre dans les centres de données et les clouds. Vous pouvez utiliser HCX pour migrer vos charges de travail VMware basées vers Amazon EVS.

Vous pouvez configurer la connectivité pour VMware HCX à l'aide Direct Connect d'une passerelle de transit associée ou à l'aide d'une AWS Site-to-Site connexion VPN à une passerelle de transit. Pour de plus amples informations, veuillez consulter Migration.

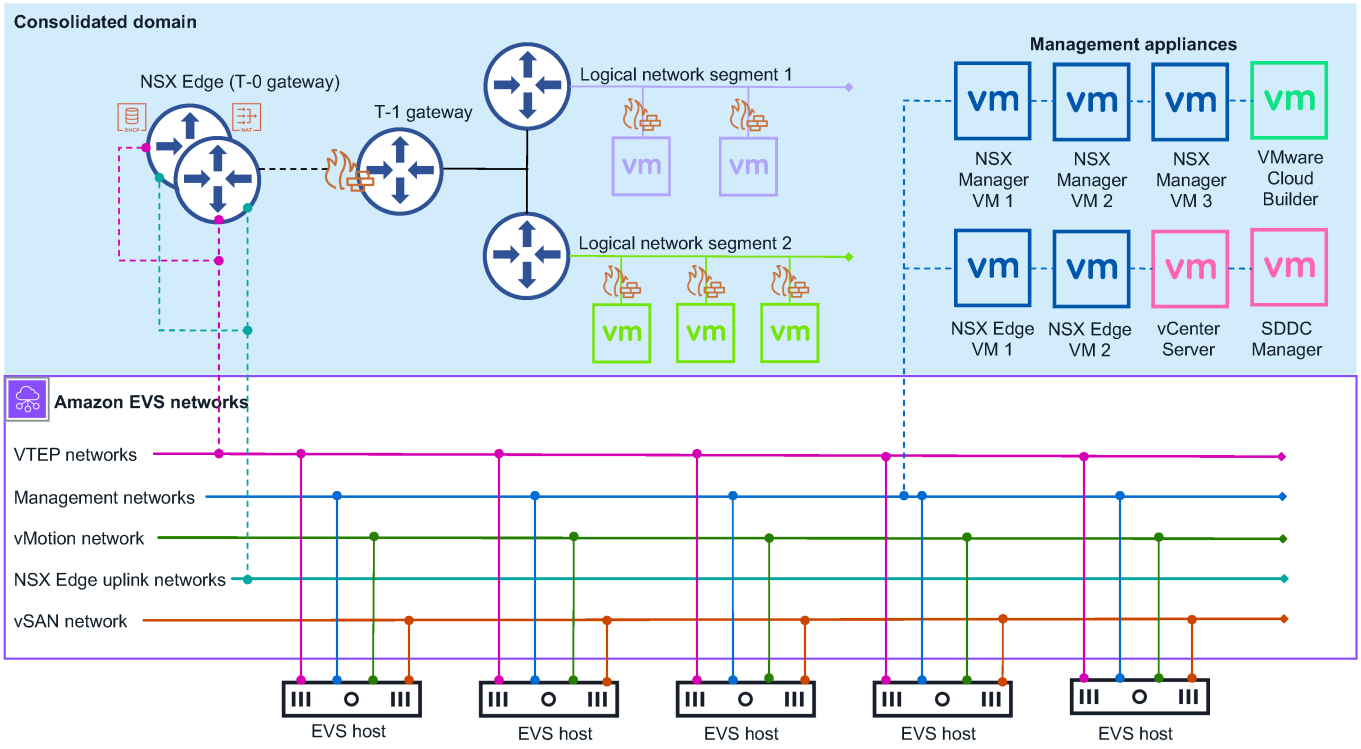
# Architecture Amazon EVS

Amazon EVS met en œuvre un modèle d'architecture consolidée VMware Cloud Foundation (VCF). Dans ce modèle, les composants de gestion VCF et les charges de travail des clients fonctionnent ensemble sur un domaine consolidé. L'environnement Amazon EVS est géré à partir d'un seul serveur vCenter avec des pools de ressources vSphere qui isolent les charges de travail de gestion et celles des clients.

Le domaine consolidé déployé par Amazon EVS contient les composants de gestion VCF suivants :

- Hôtes ESX
- Instance de vCenter Server
- Directeur du SDDC
- Banque de données vSAN
- Cluster NSX Manager à trois nœuds
- Cluster vSphere
- Cluster NSX Edge

Le schéma suivant montre un exemple d'architecture Amazon EVS déployée dans un environnement Amazon EVS et montre comment les composants de l'environnement sont connectés. Dans le diagramme, l'environnement Amazon EVS doté d'une architecture de domaine consolidée est ombré en bleu. La topologie sous-jacente du réseau Amazon EVS est illustrée par la ligne violette continue.




# Topologie du réseau

Un environnement Amazon EVS comporte deux couches de réseau de gestion distinctes :

Amazon VPC

Les sous-réseaux Amazon VPC et Amazon EVS VLAN créés dans le VPC lors de la création de l'environnement constituent le réseau sous-jacent de votre déploiement VCF. Cette infrastructure fournit une connectivité aux réseaux superposés NSX, à la gestion des hôtes, à vMotion et à VSAN. Amazon VPC Route Server permet le routage dynamique entre le réseau sous-jacent et les réseaux superposés. Pour de plus amples informations, veuillez consulter the section called "Concepts et composants".

> **Note**
>
> Les sous-réseaux VLAN Amazon EVS sont utilisés uniquement pour faciliter la communication entre sous-couches VCF. Les machines virtuelles invitées exécutant les charges de travail des clients doivent être déployées sur des réseaux superposés NSX.

Le déploiement de machines virtuelles invitées sur le réseau sous-jacent du sous-réseau Amazon EVS VLAN n'est pas pris en charge.

VMware Réseau superposé NSX

Amazon EVS configure un réseau de superposition NSX en votre nom dans le cadre du déploiement. Vous pouvez configurer des réseaux de superposition NSX supplémentaires pour isoler le réseau entre les différentes charges de travail ou applications au sein de votre environnement Amazon EVS. Pour plus d'informations, consultez la section Overlay Design for VMware Cloud Foundation dans la documentation du produit VMware Cloud Foundation.

**Note**

Amazon EVS ne prend en charge qu'une seule passerelle de niveau 0 pour un cluster Active/Standby NSX Edge comportant deux nœuds NSX Edge. Cette passerelle de niveau 0 se connecte à tous les réseaux superposés que vous configurez pour être utilisés avec Amazon EVS et en fait la publicité.

Les deux couches réseau sont connectées par un cluster Active/Standby NSX Edge avec deux nœuds NSX Edge. Les nœuds NSX Edge permettent la communication via le VPC entre les machines virtuelles VLANs du, ainsi que la connectivité Internet et la connectivité privée à Direct Connect l'aide AWS Site-to-Site d'un VPN avec une passerelle de transit.

## Considérations relatives au réseau Amazon EVS

Le réseau de gestion nécessite les configurations de ressources réseau suivantes. Vous fournissez ces entrées lors de la création de l'environnement Amazon EVS. Pour de plus amples informations, veuillez consulter the section called “Concepts et composants”.

- Un Amazon VPC. Assurez-vous que votre bloc d'adresse IPv4 CIDR VPC est dimensionné de manière appropriée pour accueillir le sous-réseau VPC et les sous-réseaux VLAN Amazon EVS requis qu'Amazon EVS provisionne lors de la création de l'environnement. Pour de plus amples informations, veuillez consulter the section called “Sous-réseau VLAN Amazon EVS”.

> **Note**
>
> Amazon EVS n'est pas compatible pour le IPv6 moment.

- Un sous-réseau d'accès aux services dans votre VPC. Amazon EVS utilise ce sous-réseau pour maintenir une connexion permanente à votre appliance SDDC Manager. Pour de plus amples informations, veuillez consulter the section called “Sous-réseau d'accès au service”.

> **Note**
>
> Amazon EVS prend uniquement en charge les déploiements mono-AZ pour le moment. Tous les sous-réseaux VPC utilisés par Amazon EVS doivent exister dans une seule zone de disponibilité dans une région où le service est disponible.

> **Note**
>
> Tous les sous-réseaux VPC nécessitent des tables de routage associées configurées conformément aux exigences réseau de votre organisation.

- Une adresse IP de serveur DNS principal et une adresse IP de serveur DNS secondaire dans l'option DHCP du VPC définie pour résoudre les adresses IP des hôtes. Amazon EVS exige également que vous créiez une zone de recherche directe DNS avec des enregistrements A et une zone de recherche inversée avec des enregistrements PTR pour chaque appliance de gestion VCF et hôte Amazon EVS de votre déploiement. Pour de plus amples informations, veuillez consulter the section called “Configuration des serveurs DNS”.
- Des blocs CIDR du sous-réseau VLAN Amazon EVS pour chaque sous-réseau VLAN qu'Amazon EVS met en service pour vous lors de la création de l'environnement. Les blocs CIDR doivent avoir une taille minimale de masque réseau /28 et une taille maximale de masque réseau /24. Les blocs CIDR ne doivent pas se chevaucher.
- Une Amazon VPC instance de serveur de route avec la propagation du serveur de route activée.
- Deux points de terminaison du serveur de routage dans le sous-réseau d'accès au service.
- Deux homologues du serveur de route qui comparent les nœuds NSX Edge qu'Amazon EVS approvisionne avec les points de terminaison du serveur de route.

### Passerelle de niveau 0

La passerelle de niveau 0 gère tout le trafic nord-sud entre les réseaux logiques et physiques et est créée sur le réseau superposé NSX. Cette passerelle de niveau 0 est créée dans le cadre du déploiement d'Amazon EVS.

> **Note**
>
> Amazon EVS ne prend en charge qu'une seule passerelle de niveau 0 pour un cluster Active/Standby NSX Edge comportant deux nœuds NSX Edge.

### Passerelle de niveau 1

La passerelle de niveau 1 gère le trafic est-ouest entre les segments de réseau routés au sein d'un environnement et est créée sur le réseau superposé NSX. La passerelle de niveau 1 possède des connexions descendantes vers des segments et des connexions montantes vers la passerelle de niveau 0. Vous pouvez créer et configurer des passerelles de niveau 1 supplémentaires si vous en avez besoin.

### Cluster NSX Edge

Amazon EVS utilise l'interface NSX Manager pour déployer un cluster NSX Edge avec deux nœuds NSX Edge qui s'exécutent en mode. Active/Standby Ce cluster NSX Edge fournit la plate-forme sur laquelle s'exécutent les passerelles de niveau 0 et de niveau 1, ainsi que les connexions IPsec VPN et leur mécanisme de routage BGP.

## Ressources Amazon EVS

Amazon EVS fournit les AWS ressources suivantes lors de la création de l'environnement. Ces ressources apparaissent dans le VPC auquel vous autorisez Amazon EVS à accéder et sont visibles dans AWS Management Console et AWS CLI après leur création.

> **Important**
>
> La modification de ces ressources en dehors de la console et de l'API Amazon EVS peut avoir un impact sur la disponibilité et la stabilité de votre environnement Amazon EVS.

- Des interfaces réseau élastiques Amazon EVS qui permettent la connectivité à vos appareils et hôtes VCF.
- Hôtes Amazon EVS ESX qui s'exécutent sur des instances Amazon EC2 bare metal. Pour de plus amples informations, veuillez consulter the section called “Hôte Amazon EVS”.

> **Important**
>
> Votre environnement Amazon EVS doit comporter au moins 4 hôtes et pas plus de 16 hôtes. Amazon EVS prend uniquement en charge les environnements de 4 à 16 hôtes.

- Sous-réseaux VLAN Amazon EVS qui connectent votre VPC aux appareils VCF. Pour de plus amples informations, veuillez consulter the section called “Sous-réseau VLAN Amazon EVS”.

# Configuration d'Amazon Elastic VMware Service

Pour utiliser Amazon EVS, vous devez configurer d'autres AWS services, ainsi que configurer votre environnement afin de répondre aux exigences de VMware Cloud Foundation (VCF). Pour une liste récapitulative des conditions préalables au déploiement, voir. the section called “Liste de contrôle pour le déploiement”

Rubriques



## Inscrivez-vous pour AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

1. Ouvrez l' https://portal.aws.amazon.com/billing/inscription.

2. Suivez les instructions en ligne.

## Créer un utilisateur IAM

1. Connectez-vous à la console IAM en tant que propriétaire du compte en choisissant Utilisateur root et en saisissant l'adresse e-mail de votre AWS compte. Sur la page suivante, saisissez votre mot de passe.

> **Note**
>
> Nous vous recommandons vivement de respecter la bonne pratique qui consiste à avoir recours à l'utilisateur IAM `Administrator` ci-dessous et protéger les informations d'identification de l'utilisateur racine. Connectez-vous en tant qu'utilisateur principal pour effectuer certaines tâches de gestion du compte et du service.

2. Dans le volet de navigation, sélectionnez Utilisateurs, puis sélectionnez Créer un utilisateur.
3. Dans User name (Nom d'utilisateur), saisissez `Administrator`.
4. Cochez la case à côté de l'accès à AWS la console de gestion. Ensuite, sélectionnez Custom password (Mot de passe personnalisé), puis saisissez votre nouveau mot de passe dans la zone de texte.
5. (Facultatif) Par défaut, le nouvel utilisateur AWS doit créer un nouveau mot de passe lors de sa première connexion. Désélectionnez la case en regard de User must create a new password at next sign in (L'utilisateur doit créer un nouveau mot de passe à sa prochaine connexion) pour autoriser le nouvel utilisateur à réinitialiser son mot de passe une fois qu'il s'est connecté.
6. Sélectionnez Next: Permissions (Étape suivante : autorisations).
7. Sous Set permissions (Définir des autorisations), choisissez Add user to group (Ajouter un utilisateur au groupe).
8. Choisissez Créer un groupe.
9. Dans la boîte de dialogue Create group (Créer un groupe), pour Group name (Nom du groupe), saisissez `Administrators`.
10. Choisissez Filtrer les politiques, puis sélectionnez la fonction AWS managed -job pour filtrer le contenu du tableau.
11. Dans la liste des politiques, cochez la case correspondant à AdministratorAccess. Choisissez ensuite Create group (Créer un groupe).

> **Note**
>
> Vous devez activer l'accès des utilisateurs et des rôles IAM à Billing avant de pouvoir utiliser les `AdministratorAccess` autorisations pour accéder à la console AWS Billing and Cost Management. Pour ce faire, suivez les instructions de l'étape 1 du didacticiel sur la délégation de l'accès à la console de facturation.

12. De retour dans la liste des groupes, activez la case à cocher du nouveau groupe. Choisissez Refresh (Actualiser) si nécessaire pour afficher le groupe dans la liste.
13. Choisissez Next: Tags (Suivant : Étiquettes).
14. (Facultatif) Ajoutez des métadonnées à l'utilisateur en associant les balises sous forme de paires clé-valeur. Pour plus d'informations sur l'utilisation des identifications dans IAM, consultez Étiquetage des entités IAM dans le Guide de l'utilisateur IAM.
15. Choisissez Next: Review (Suivant : Vérification) pour afficher la liste des membres du groupe à ajouter au nouvel utilisateur. Une fois que vous êtes prêt à continuer, choisissez Create user (Créer un utilisateur).

Vous pouvez utiliser ce même processus pour créer davantage de groupes et d'utilisateurs et pour donner à vos utilisateurs l'accès aux ressources de votre AWS compte. Pour en savoir plus sur l'utilisation de politiques qui limitent les autorisations des utilisateurs à AWS des ressources spécifiques, voir Gestion des accès et exemples de politiques.

## Créez un rôle IAM pour déléguer l'autorisation Amazon EVS à un utilisateur IAM

Vous pouvez utiliser des rôles pour déléguer l'accès à vos AWS ressources. Avec les rôles IAM, vous pouvez établir des relations de confiance entre votre compte de confiance et d'autres comptes de AWS confiance. Le compte de confiance possède la ressource à laquelle accéder, et le compte de confiance contient les utilisateurs qui ont besoin d'accéder à la ressource.

Une fois que vous avez créé la relation de confiance, un utilisateur IAM ou une application du compte sécurisé peut utiliser l'opération d'`AssumeRole`API AWS Security Token Service (AWS STS). Cette opération fournit des informations de sécurité temporaires qui permettent d'accéder aux AWS ressources de votre compte. Pour plus d'informations, consultez la section Créer un rôle pour

déléguer des autorisations à un utilisateur IAM dans le Guide de l' Gestion des identités et des accès AWS utilisateur.

Suivez ces étapes pour créer un rôle IAM avec une politique d'autorisation qui autorise l'accès aux opérations Amazon EVS.

> **Note**
>
> Amazon EVS ne prend pas en charge l'utilisation d'un profil d'instance pour transmettre un rôle IAM à une EC2 instance.

Example

IAM console

1. Accédez à la console IAM.
2. Dans le menu de gauche, sélectionnez Politiques.
3. Choisissez Create Policy (Créer une politique).
4. Dans l'éditeur de politique, créez une politique d'autorisation qui active les opérations Amazon EVS. Pour un exemple de politique, consultez the section called “Création et gestion d'un environnement Amazon EVS”. Pour consulter toutes les actions, ressources et clés de condition Amazon EVS disponibles, consultez la section Actions de la référence d'autorisation de service.
5. Choisissez Suivant.
6. Sous Nom de la politique, entrez un nom de politique significatif pour identifier cette stratégie.
7. Passez en revue les autorisations définies dans cette politique.
8. (Facultatif) Ajoutez des balises pour identifier, organiser ou rechercher cette ressource.
9. Choisissez Create Policy (Créer une politique).
10. Dans le menu de gauche, choisissez Rôles.
11. Choisissez Créer un rôle.
12. Pour Type d'entité de confiance, sélectionnez Compte AWS.
13. Sous An Compte AWS , spécifiez le compte sur lequel vous souhaitez effectuer des actions Amazon EVS et choisissez Next.

14. Sur la page Ajouter des autorisations, sélectionnez la politique d'autorisation que vous avez créée précédemment et choisissez Suivant.
15. Sous Nom du rôle, entrez un nom significatif pour identifier ce rôle.
16. Passez en revue la politique de confiance et assurez-vous que le bon Compte AWS est indiqué comme principal.
17. (Facultatif) Ajoutez des balises pour identifier, organiser ou rechercher cette ressource.
18. Choisissez Créer un rôle.

AWS CLI

1. Copiez le contenu suivant dans un fichier JSON de politique de confiance. Pour l'ARN principal, remplacez l' Compte AWS ID et le `service-user` nom d'exemple par vos propres Compte AWS ID et nom d'utilisateur IAM.

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

2. Créez le rôle. `evs-environment-role-trust-policy.json`Remplacez-le par le nom de votre fichier de politique de confiance.

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

3. Créez une politique d'autorisation qui active les opérations Amazon EVS et associez la politique au rôle. Remplacez `myAmazonEVSEnvironmentRole` par le nom de votre rôle. Pour un exemple de politique, consultez the section called “Création et gestion d'un environnement Amazon EVS”. Pour consulter toutes les actions, ressources et clés de condition Amazon EVS disponibles, consultez la section Actions de la référence d'autorisation de service.

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

## Souscrivez à un AWS plan Business, AWS Enterprise On-Ramp ou AWS Enterprise Support

Amazon EVS exige que les clients soient inscrits à un plan AWS Business, AWS Enterprise On-Ramp ou Enterprise AWS Support pour bénéficier d'un accès continu au support technique et aux conseils architecturaux. AWS Business Support est le niveau de AWS support minimum qui répond aux exigences d'Amazon EVS. Si vous avez des charges de travail critiques, nous vous recommandons de souscrire aux plans Enterprise On-Ramp ou AWS AWS Enterprise Support. Pour plus d'informations, consultez la section Comparer les plans de AWS support.

> **Important**
>
> La création de l'environnement Amazon EVS échoue si vous ne souscrivez pas à un AWS plan Business, AWS Enterprise On-Ramp ou Enterprise AWS Support.

## Vérifiez les quotas

Pour permettre la création d'un environnement Amazon EVS, assurez-vous que votre compte dispose des quotas minimaux requis au niveau du compte. Pour de plus amples informations, veuillez consulter Quotas de service.

> **Important**
>
> La création de l'environnement Amazon EVS échoue si le nombre d'hôtes par valeur de quota d'environnement EVS n'est pas d'au moins 4.

## Planifier les tailles de CIDR VPC

Lorsque vous créez un environnement Amazon EVS, vous devez spécifier un bloc d'adresse CIDR VPC. Le bloc d'adresse CIDR VPC ne peut pas être modifié une fois l'environnement créé et doit

disposer de suffisamment d'espace réservé pour accueillir les sous-réseaux EVS et les hôtes requis créés par Amazon EVS lors du déploiement de l'environnement. Par conséquent, il est essentiel de planifier soigneusement la taille des blocs CIDR, en tenant compte des exigences d'Amazon EVS et de vos futurs besoins de dimensionnement avant le déploiement. Amazon EVS nécessite un bloc d'adresse CIDR VPC d'une taille minimale de masque réseau /22 afin de laisser suffisamment d'espace pour les sous-réseaux et hôtes EVS requis. Pour de plus amples informations, veuillez consulter the section called “Considérations relatives au réseau Amazon EVS”.

> **Important**
>
> Assurez-vous de disposer d'un espace d'adresse IP suffisant pour votre sous-réseau VPC et pour les sous-réseaux VLAN créés par Amazon EVS pour les appliances VCF. Le bloc d'adresse CIDR VPC doit avoir une taille minimale de masque réseau /22 pour laisser suffisamment d'espace aux sous-réseaux et hôtes EVS requis.

> **Note**
>
> Amazon EVS n'est pas compatible pour le IPv6 moment.

## Création d'un VPC avec des sous-réseaux

Amazon EVS déploie votre environnement dans un VPC que vous fournissez. Ce VPC doit contenir un sous-réseau pour l'accès au service Amazon EVS (). the section called “Sous-réseau d’accès au service” Pour savoir comment créer un VPC avec des sous-réseaux pour Amazon EVS, consultez. the section called “Création d'un VPC avec des sous-réseaux et des tables de routage”

## Configuration de la table de routage principale du VPC

Les sous-réseaux VLAN Amazon EVS sont implicitement associés à la table de routage principale du VPC. Pour permettre la connectivité aux services dépendants tels que le DNS ou les systèmes sur site afin de réussir le déploiement de l'environnement, vous devez configurer la table de routage principale pour autoriser le trafic vers ces systèmes. Pour de plus amples informations, veuillez consulter the section called “Associez explicitement des sous-réseaux VLAN Amazon EVS à une table de routage VPC”.

> **Important**
>
> Amazon EVS prend en charge l'utilisation d'une table de routage personnalisée uniquement après la création de l'environnement Amazon EVS. Les tables de routage personnalisées ne doivent pas être utilisées lors de la création de l'environnement Amazon EVS, car cela peut entraîner des problèmes de connectivité.

## Exigences relatives aux itinéraires de passerelle

Configurez les itinéraires pour ces types de passerelles en fonction de vos besoins en matière de connectivité :

- Passerelle NAT (NGW)
  - Facultatif pour l'accès Internet sortant uniquement.
  - Doit se trouver dans un sous-réseau public avec accès à une passerelle Internet.
  - Ajoutez des routes à partir de sous-réseaux privés et de sous-réseaux VLAN EVS à la passerelle NAT.
  - Pour plus d'informations, consultez la section Travailler avec des passerelles NAT dans le guide de l'utilisateur Amazon VPC.
- Passerelle de transit (TGW)
  - Nécessaire pour la connectivité sur site via AWS Direct Connect et AWS Site-to-Site VPN.
  - Ajoutez des itinéraires pour les plages de réseaux sur site.
  - Configurez la propagation de l'itinéraire si vous utilisez BGP.
  - Pour plus d'informations, consultez la section Passerelles de transit dans Amazon VPC Transit Gateways dans le guide de l'utilisateur Amazon VPC.

## Bonnes pratiques

- Documentez toutes les configurations de table de routage.
- Utilisez des conventions de dénomination cohérentes.
- Auditez régulièrement vos tables de routage.
- Testez la connectivité après avoir apporté des modifications.
- Sauvegardez les configurations des tables de routage.

- Surveillez l'état de l'itinéraire et la propagation.

Pour plus d'informations sur l'utilisation des tables de routage, consultez Configurer les tables de routage dans le guide de l'utilisateur Amazon VPC.

## Configurez le jeu d'options DHCP de votre VPC

**Important**

Le déploiement de votre environnement échoue si vous ne répondez pas aux exigences Amazon EVS suivantes :

- Incluez une adresse IP de serveur DNS principal et une adresse IP de serveur DNS secondaire dans le jeu d'options DHCP.
- Incluez une zone de recherche directe DNS avec des enregistrements A pour chaque appliance de gestion VCF et hôte Amazon EVS de votre déploiement.
- Incluez une zone de recherche inversée DNS avec des enregistrements PTR pour chaque appliance de gestion VCF et hôte Amazon EVS de votre déploiement.
- Configurez la table de routage principale du VPC pour vous assurer qu'il existe une route vers vos serveurs DNS.
- Assurez-vous que l'enregistrement de votre nom de domaine est valide et n'a pas expiré, et qu'il n'existe pas de nom d'hôte ou d'adresse IP en double.
- Configurez vos groupes de sécurité et vos listes de contrôle d'accès réseau (ACLs) pour permettre à Amazon EVS de communiquer avec :
  - Serveurs DNS via TCP/UDP le port 53.
  - Sous-réseau VLAN de gestion de l'hôte via HTTPS et SSH.
  - Sous-réseau VLAN de gestion via HTTPS et SSH.

Pour de plus amples informations, veuillez consulter the section called "Configuration des serveurs DNS et NTP à l'aide du jeu d'options DHCP du VPC".

# Création et configuration de l'infrastructure du serveur de routage VPC

Amazon EVS utilise Amazon VPC Route Server pour activer le routage dynamique basé sur le BGP vers votre réseau sous-jacent VPC. Vous devez spécifier un serveur de routage qui partage des itinéraires vers au moins deux points de terminaison du serveur de routage dans le sous-réseau d'accès au service. L'ASN pair configuré sur les pairs du serveur de routage doit correspondre et les adresses IP des pairs doivent être uniques.

**Important**

Le déploiement de votre environnement échoue si vous ne répondez pas aux exigences Amazon EVS suivantes pour la configuration du serveur de routage VPC :

- Vous devez configurer au moins deux points de terminaison du serveur de routage dans le sous-réseau d'accès au service.
- Lors de la configuration du protocole BGP (Border Gateway Protocol) pour la passerelle de niveau 0, la valeur ASN du pair du serveur de routage VPC doit correspondre à la valeur ASN du pair NSX Edge.
- Lorsque vous créez les deux homologues du serveur de routage, vous devez utiliser une adresse IP unique provenant du VLAN de liaison montante NSX pour chaque point de terminaison. Ces deux adresses IP seront attribuées aux NSX Edge lors du déploiement de l'environnement Amazon EVS.
- Lorsque vous activez la propagation par le serveur de routage, vous devez vous assurer que toutes les tables de routage propagées possèdent au moins une association de sous-réseau explicite. La publicité de route BGP échoue si les tables de routage propagées n'ont pas d'association de sous-réseau explicite.

**Note**

Pour la détection de la réactivité entre pairs du serveur Route, Amazon EVS prend uniquement en charge le mécanisme BGP keepalive par défaut. Amazon EVS ne prend pas en charge la détection du transfert bidirectionnel (BFD) à sauts multiples.

## Conditions préalables

Avant de commencer, vous avez besoin des éléments suivants :

- Un sous-réseau VPC pour votre serveur de routage.
- Autorisations IAM pour gérer les ressources du serveur de routage VPC.
- Une valeur ASN BGP pour le serveur de route (ASN côté Amazon). Cette valeur doit se situer dans la plage 1-4294967295.
- Un ASN homologue pour associer votre serveur de routage à la passerelle NSX Tier-0. Les valeurs ASN homologues saisies dans le serveur de routage et la passerelle NSX Tier-0 doivent correspondre. L'ASN par défaut pour un dispositif NSX Edge est 65000.

## Étapes

Pour connaître les étapes de configuration du serveur de routage VPC, consultez le didacticiel de démarrage du serveur de routage.

> **Note**
>
> Si vous utilisez une passerelle NAT ou une passerelle de transit, assurez-vous que votre serveur de routage est correctement configuré pour propager les routes NSX vers les tables de routage VPC.

> **Note**
>
> Nous vous recommandons d'activer les itinéraires persistants pour l'instance du serveur de routage avec une durée de persistance comprise entre 1 et 5 minutes. Si cette option est activée, les itinéraires seront conservés dans la base de données de routage du serveur de routage même si toutes les sessions BGP se terminent.

> **Note**
>
> L'état de connectivité BGP sera indisponible jusqu'à ce que l'environnement Amazon EVS soit déployé et opérationnel.

# Création d'une passerelle de transit pour la connectivité sur site

Vous pouvez configurer la connectivité entre votre centre de données sur site et votre AWS infrastructure à l'aide Direct Connect d'une passerelle de transit associée ou d'une AWS Site-to-Site connexion VPN à une passerelle de transit. Pour de plus amples informations, veuillez consulter the section called "Configuration de la connectivité réseau sur site (facultatif)".

# Créer une réservation Amazon EC2 Capacity

Amazon EVS lance des instances Amazon EC2 i4i.metal qui représentent les hôtes ESX dans votre environnement Amazon EVS. Pour vous assurer de disposer d'une capacité d'instance i4i.metal suffisante lorsque vous en avez besoin, nous vous recommandons de demander une réservation Amazon EC2 Capacity. Vous pouvez créer une réserve de capacité à tout moment, et vous pouvez choisir la date à laquelle elle commence. Vous pouvez demander une réservation de capacité pour une utilisation immédiate, ou vous pouvez demander une réservation de capacité pour une date future. Pour plus d'informations, consultez la section Réserver une capacité de calcul avec des réservations de capacité EC2 à la demande dans le guide de l'utilisateur d'Amazon Elastic Compute Cloud.

# Configurez le AWS CLI

AWS CLI Il s'agit d'un outil de ligne de commande permettant de travailler avec Services AWS, notamment, Amazon EVS. Il est également utilisé pour authentifier les utilisateurs ou les rôles IAM afin d'accéder à l'environnement de virtualisation Amazon EVS et à d'autres AWS ressources depuis votre machine locale. Pour provisionner AWS des ressources à partir de la ligne de commande, vous devez obtenir un ID de clé d' AWS accès et une clé secrète à utiliser dans la ligne de commande. Vous devez ensuite configurer ces informations d'identification dans l' AWS CLI. Pour plus d'informations, voir Configurer le AWS CLI dans le guide de l' AWS Command Line Interface utilisateur pour la version 2.

# Création d'une paire de Amazon EC2 clés

Amazon EVS utilise une paire de Amazon EC2 clés que vous fournissez lors de la création de l'environnement pour vous connecter à vos hôtes. Pour créer une paire de clés, suivez les étapes décrites dans la section Créer une paire de clés pour votre Amazon EC2 instance dans le Guide de Amazon Elastic Compute Cloud l'utilisateur.

# Préparez votre environnement pour VMware Cloud Foundation (VCF)

Avant de déployer votre environnement Amazon EVS, celui-ci doit répondre aux exigences de l'infrastructure VMware Cloud Foundation (VCF). Pour connaître les prérequis détaillés du VCF, consultez le manuel de planification et de préparation dans la documentation du produit VMware Cloud Foundation.

Vous devez également vous familiariser avec les exigences de VCF 5.2.x. Consultez les notes de mise à jour de VCF 5.2.x pour obtenir des informations de version pertinentes.

> **Note**
>
> Pour plus d'informations sur les versions VCF fournies par Amazon EVS, consultez. the section called "Versions et EC2 instances VCF"

## Acquisition de clés de licence VCF

Pour utiliser Amazon EVS, vous devez fournir une clé de solution VCF et une clé de licence vSAN. La clé de solution VCF doit comporter au moins 256 cœurs. La clé de licence vSAN doit avoir au moins 110 TiB de capacité vSAN. Pour plus d'informations sur les licences VCF, consultez la section Gestion des clés de licence dans VMware Cloud Foundation dans le guide d'administration de VMware Cloud Foundation.

> **Important**
>
> Utilisez l'interface utilisateur du SDDC Manager pour gérer la solution VCF et les clés de licence vSAN. Amazon EVS exige que vous conserviez des clés de solution VCF et de licence vSAN valides dans SDDC Manager pour que le service fonctionne correctement.

> **Note**
>
> Votre licence VCF sera mise à la disposition d'Amazon EVS dans toutes les AWS régions pour garantir la conformité des licences. Amazon EVS ne valide pas les clés de licence. Pour valider les clés de licence, consultez le support de Broadcom.

# VMware Prérequis HCX

Vous pouvez utiliser VMware HCX pour migrer vos charges de travail VMware existantes vers Amazon EVS. Avant d'utiliser VMware HCX avec Amazon EVS, assurez-vous que les tâches préalables suivantes ont été effectuées.

> **Note**
>
> VMware HCX n'est pas installé dans l'environnement EVS par défaut.

- Avant de pouvoir utiliser VMware HCX avec Amazon EVS, les exigences minimales en matière de sous-couche réseau doivent être satisfaites. Pour plus d'informations, consultez la section Configuration minimale requise pour la sous-couche réseau dans le guide de l'utilisateur du VMware HCX.
- Vérifiez que VMware NSX est installé et configuré dans l'environnement. Pour plus d'informations, consultez le guide d'installation de VMware NSX.
- Assurez-vous que VMware HCX est activé et installé dans l'environnement. Pour plus d'informations sur l'activation et l'installation de VMware HCX, voir À propos de la mise en route avec VMware HCX dans le guide de démarrage avec VMware HCX.
- Si vous avez besoin d'une connexion Internet HCX, vous devez effectuer les tâches préalables suivantes :
  - Assurez-vous que votre quota IPAM pour la longueur du masque réseau de blocs IPv4 CIDR publics contigus fourni par Amazon est de /28 ou plus.

    > **Important**
    >
    > Pour la connectivité Internet HCX, Amazon EVS nécessite l'utilisation d'un bloc IPv4 CIDR provenant d'un pool IPAM public avec une longueur de masque réseau de /28 ou plus. L'utilisation de n'importe quel bloc CIDR dont la longueur du masque réseau est inférieure à /28 entraînera des problèmes de connectivité HCX. Pour plus d'informations sur l'augmentation des quotas IPAM, consultez la section Quotas pour votre IPAM.

  - Créez un pool IPAM et un pool IPv4 IPAM public avec un CIDR dont la longueur de masque réseau minimale est de /28.

- Allouez au moins deux adresses IP élastiques (EIPs) depuis le pool IPAM pour les appliances HCX Manager et HCX Interconnect (HCX-IX). Allouez une adresse IP élastique supplémentaire pour chaque appliance réseau HCX que vous devez déployer.
- Ajoutez le bloc d'adresse IPv4 CIDR public en tant que CIDR supplémentaire à votre VPC.

Pour plus d'informations sur la configuration de HCX, reportez-vous aux sections the section called "Choisissez votre option de connectivité HCX" etthe section called "Options de connectivité HCX".

# Liste de contrôle préalable au déploiement d'Amazon EVS

Cette section contient une liste des conditions préalables qui doivent être remplies pour permettre un déploiement réussi de l'environnement Amazon EVS.

Informations sur la clé de licence VCF

| Composant | Description | Configuration requise | Exemple de valeur (s) |
|---|---|---|---|
| Identifiant du site | ID de site fourni par Broadcom pour accéder au portail d'assistance de Broadcom. | Vous devez fournir un identifiant de site de Broadcom dans la demande de création de l'environnement EVS. | 01234567 |
| Clé de solution VCF | Une clé de licence VCF unique qui déverrouille les fonctionnalités de l'ensemble de la pile VCF, notamment vSphere, NSX, SDDC Manager et vCenter Server. | Vous devez fournir une clé de solution VCF active valide dans la demande de création de l'environnement EVS. La clé ne peut pas déjà être utilisée par un environnement EVS existant. | ABCDE-FGHIJ-KLMNO-PQRSTU-VWXYZ |
| Clé de licence vSAN | Une clé de licence vSAN vous permet d'activer et d'utiliser le | Vous devez fournir une clé de licence vSAN active valide | ABCDE-FGHIJ-KLMNO-PQRSTU-VWXYZ |

| Composant | Description | Configuration requise | Exemple de valeur (s) |
| --- | --- | --- | --- |
| | logiciel vSAN dans un environnement VCF. | dans la demande de création de l'environnement EVS. La clé ne peut pas déjà être utilisée par un environnement EVS existant. | |

AWS informations sur le compte et la région

| Composant | Description | Configuration requise | Exemple de valeur (s) |
| --- | --- | --- | --- |
| AWS numéro d'identification du compte | Le AWS compte vous permet de créer et de gérer AWS des ressources et des AWS services d'accès. | Doit avoir accès à un AWS compte. | 999999999999 |
| AWS Région | Zone géographique physique dans laquelle se AWS trouvent plusieurs centres de données isolés appelés zones de disponibilité. | Vous devez spécifier une AWS région dans laquelle Amazon EVS doit être déployé. Pour obtenir la liste des régions dans lesquelles Amazon EVS est actuellement disponible, consultez la section Points de terminaison et quotas Amazon Elastic VMware Service dans le Guide de référence AWS général. | USA Ouest (Oregon) |

AWS Transit Gateway pour la connectivité des centres de données sur site

| Composant | Description | Configuration requise | Exemple (s) de valeur |
|---|---|---|---|
| ID de passerelle de transit | Une passerelle de transit agit comme un routeur virtuel régional pour le trafic circulant entre votre VPC et les réseaux locaux. | Vous devez utiliser une passerelle de transit pour connecter un environnement Amazon EVS à vos réseaux locaux. | TGW-0262A0E521 Exemple |
| Méthode de connectivité | Pour connecter vos réseaux locaux à un environnement Amazon EVS, vous devez utiliser une passerelle de transit avec Direct AWS Connect ou AWS Site-to-Site VPN. | Déterminez si vous allez utiliser AWS Direct Connect, un AWS Site-to-Site VPN ou une combinaison des deux. Pour plus d'informations sur l'utilisation d' Site-to-Siteun VPN avec Direct Connect, consultez la section AWS Site-to-Site VPN IP privé avec AWS Direct Connect. | AWS Site-to-Site VPN avec AWS Direct Connect |

VPC pour environnement Amazon EVS

| Composant | Description | Configuration requise | Exemple (s) de valeur |
|---|---|---|---|
| ID du VPC | Un VPC est un réseau virtuel qui ressemble beaucoup à un réseau traditionnel que vous exploiteriez dans votre propre centre de données. | N'importe quel Amazon VPC peut être utilisé pour le déploiement de l'environnement. | vpc-0abcdef1234567890 |

| Composant | Description | Configuration requise | Exemple (s) de valeur |
| --- | --- | --- | --- |
| Bloc d'adresse CIDR VPC | Dans Amazon VPC, un bloc CIDR définit la plage d'adresses IP disponibles au sein de votre VPC. | Un bloc d'adresse CIDR RFC 1918 avec une taille minimale de masque réseau /22. Le bloc d'adresse CIDR VPC doit être dimensionné de manière appropriée pour accueillir tous les sous-réseaux et hôtes EVS à déployer dans votre VPC. Ce bloc CIDR doit être unique dans tous vos environnements. | 10,1.0.0/20 |

Sous-réseaux VPC pour environnement EVS

| Composant | Description | Configuration requise | Exemple (s) de valeur |
| --- | --- | --- | --- |
| ID de sous-réseau d'accès au service | Un sous-réseau d'accès aux services est un sous-réseau VPC standard qui permet d'accéder aux services Amazon EVS. Pour de plus amples informations, veuillez consulter the section called "Sous-réseau d'accès au service". | N'importe quel sous-réseau VPC peut être utilisé, à condition que la taille du sous-réseau soit appropriée au sein du VPC. Nous vous suggérons de spécifier un bloc CIDR de sous-réseau VPC avec un masque réseau /24. | sous-net-abcdef1234567890e |
| sous-réseau d'accès aux services CIDR | un bloc CIDR de sous-réseau VPC est | Le sous-réseau d'accès au service | 10.1.0.0/24 |

| Composant | Description | Configuration requise | Exemple (s) de valeur |
| --- | --- | --- | --- |
| | une plage d'adresses IP, définie à l'aide de la notation CIDR, qui est allouée à un sous-réseau spécifique au sein d'un VPC. | doit être dimensionné de manière appropriée pour accueillir également les autres sous-réseaux et hôtes EVS à déployer dans votre VPC. Nous vous suggérons de spécifier un bloc CIDR de sous-réseau VPC avec un masque réseau /24. | |
| AWS ID de zone de disponibilité dans la région | Emplacement distinct au sein d'une AWS région, conçu pour être isolé des défaillances survenant dans une autre région AZs, et composé d'un ou de plusieurs centres de données. | Vous pouvez spécifier la zone de disponibilité dans laquelle les sous-réseaux VPC sont déployés lors de leur création. Pour plus d'informations, consultez la section Créer un sous-réseau dans le guide de l'utilisateur Amazon VPC. | us-west-2a |

Sous-réseaux VLAN EVS pour environnement EVS

| Composant | Description | Configuration requise | Exemple (s) de valeur |
| --- | --- | --- | --- |
| Gestion de l'hôte (VLAN) (CIDR) | Le bloc CIDR pour le sous-réseau VLAN de gestion de l'hôte. Pour de plus amples informations, veuillez | Le masque de réseau doit avoir une taille minimale de /28 et une taille maximale de masque de | 10,1.1.0/24 |

| Composant | Description | Configuration requise | Exemple (s) de valeur |
|---|---|---|---|
| | consulter the section called "Sous-réseau VLAN de gestion de l'hôte". | réseau /24. Il ne doit pas se chevaucher avec un bloc CIDR existant associé au VPC. | |
| CIDR VLAN vMotion | Le bloc CIDR pour le sous-réseau VLAN vMotion. Pour de plus amples informations, veuillez consulter the section called "Sous-réseau VLAN vMotion". | Doit être de la même taille que le VLAN de gestion de l'hôte. | 10,1.2,0/24 |
| CIDR VLAN vSAN | Le bloc CIDR pour le sous-réseau VLAN vSAN. Pour de plus amples informations, veuillez consulter the section called "Sous-réseau VLAN vSAN". | Doit être de la même taille que le VLAN de gestion de l'hôte. | 10,1.3,0/24 |
| VTEP VLAN CIDR | Le bloc CIDR pour le sous-réseau VLAN VTEP. Pour de plus amples informations, veuillez consulter the section called "Sous-réseau VLAN VTEP". | Doit être de la même taille que le VLAN de gestion de l'hôte. | 10.1.4.0/24 |

| Composant | Description | Configuration requise | Exemple (s) de valeur |
|---|---|---|---|
| VLAN VTEP Edge (CIDR) | Le bloc CIDR pour le sous-réseau VLAN VTEP Edge. Pour de plus amples informations, veuillez consulter the section called "Sous-réseau VLAN VTEP Edge". | Le masque de réseau doit avoir une taille minimale de /28 et une taille maximale de masque de réseau /24. Il ne doit pas se chevaucher avec un bloc CIDR existant associé au VPC. | 10,1,5,0/24 |
| VM de gestion, VLAN, CIDR | Le bloc CIDR pour le sous-réseau VLAN de la machine virtuelle de gestion. Pour de plus amples informations, veuillez consulter the section called "Sous-réseau VLAN de la machine virtuelle de gestion". | Le masque de réseau doit avoir une taille minimale de /28 et une taille maximale de masque de réseau /24. Il ne doit pas se chevaucher avec un bloc CIDR existant associé au VPC. | 10,1,6,0/24 |
| VLAN à liaison montante HCX CIDR | Le bloc CIDR pour le sous-réseau VLAN à liaison montante HCX. Pour de plus amples informations, veuillez consulter the section called "Sous-réseau VLAN à liaison montante HCX". | Le masque de réseau doit avoir une taille minimale de /28 et une taille maximale de masque de réseau /24. Il ne doit pas se chevaucher avec un bloc CIDR existant associé au VPC. | 10,1.7,0/24 |

| Composant | Description | Configuration requise | Exemple (s) de valeur |
|---|---|---|---|
| CIDR VLAN NSX Uplink | Le bloc CIDR pour le sous-réseau VLAN NSX Uplink. Pour de plus amples informations, veuillez consulter the section called "Sous-réseau VLAN NSX Uplink". | Le masque de réseau doit avoir une taille minimale de /28 et une taille maximale de masque de réseau /24. Il ne doit pas se chevaucher avec un bloc CIDR existant associé au VPC. | 10,1,8,0/24 |
| VLAN d'extension 1 CIDR | Bloc CIDR pour le sous-réseau VLAN d'extension. Pour de plus amples informations, veuillez consulter the section called "Sous-réseau VLAN d'extension". | Le masque de réseau doit avoir une taille minimale de /28 et une taille maximale de masque de réseau /24. Il ne doit pas se chevaucher avec un bloc CIDR existant associé au VPC. | 10,1.9,0/24 |
| VLAN d'extension 2 CIDR | Bloc CIDR pour le sous-réseau VLAN d'extension. Pour de plus amples informations, veuillez consulter the section called "Sous-réseau VLAN d'extension". | Le masque de réseau doit avoir une taille minimale de /28 et une taille maximale de masque de réseau /24. Il ne doit pas se chevaucher avec un bloc CIDR existant associé au VPC. | 10,1.10,0/24 |

Infrastructure DNS et NTP

| Composant | Description | Configuration requise | Exemple (s) de valeur |
| --- | --- | --- | --- |
| Adresse IP du serveur DNS principal | Le serveur DNS (Domain Name System) principal utilisé comme source de vérité pour tous les enregistrements DNS du domaine. | Vous pouvez utiliser n'importe quelle IPv4 adresse valide et non utilisée comprise dans la plage d'hôtes utilisables. | 10.1.1.10 |
| Adresse IP du serveur DNS secondaire | Un serveur DNS de sauvegarde pour les enregistrements DNS du domaine. | Vous pouvez utiliser n'importe quelle IPv4 adresse valide et non utilisée comprise dans la plage d'hôtes utilisables. | 10,15,25 |
| Adresse IP du serveur NTP | Un serveur NTP (Network Time Protocol) est un appareil ou une application qui synchronise les horloges au sein d'un réseau à l'aide de la norme NTP. | Vous pouvez utiliser le service Amazon Time Sync par défaut avec l'adresse `169.254.169.123` IP locale ou une autre adresse IP du serveur NTP. | 169.254.169.123 (service Amazon Time Sync) |
| FQDN pour le déploiement de VCF | Un nom de domaine complet (FQDN) est le nom absolu d'un appareil sur un réseau. Un FQDN se compose d'un nom d'hôte et d'un nom de domaine. | Un FQDN ne peut contenir que des caractères alphanumériques, le signe moins (-) et des points qui servent de délimiteur entre les libellés. Il doit s'agir d'un FQDN | evs.local |

| Composant | Description | Configuration requise | Exemple (s) de valeur |
| --- | --- | --- | --- |
| | | unique valide et non expiré. | |

Ensemble d'options DHCP VPC

| Composant | Description | Configuration requise | Exemple (s) de valeur |
| --- | --- | --- | --- |
| ID du jeu d'options DHCP | Un ensemble d'options DHCP est un groupe de paramètres réseau utilisés par les ressources de votre VPC, EC2 telles que les instances, pour communiquer sur votre réseau virtuel. | Doit contenir au moins 2 serveurs DNS. Vous pouvez utiliser Route 53 ou des serveurs DNS personnalisés. Doit également contenir votre nom de domaine DNS et un serveur NTP. | dopt-0a1b2c3d |

EC2 paire de clés

| Composant | Description | Configuration requise | Exemple (s) de valeur |
| --- | --- | --- | --- |
| EC2 nom de la paire de clés | Une paire de EC2 clés est un ensemble d'informations de sécurité utilisées pour se connecter en toute sécurité à une EC2 instance Amazon. | Le nom de la paire de clés doit être unique. | `my-ec2-key-pair` |

Tables de routage de VPC

| Composant | Description | Configuration requise | Exemple (s) de valeur |
| --- | --- | --- | --- |
| ID de la table de routage principale | Dans Amazon VPC, la table de routage principale est la table de routage par défaut créée automatiquement avec le VPC. Elle régit le trafic pour tous les sous-réseaux VPC qui ne sont pas explicitement associés à une autre table de routage. Les sous-réseaux VLAN EVS sont implicitement associés à la table de routage principale de votre VPC lorsqu'Amazon EVS les crée. | Doit être configuré pour permettre la connectivité aux services dépendants tels que le DNS ou les systèmes sur site pour que le déploiement de l'environnement soit réussi. | rtb-0123456789abcdef0 |

Liste de contrôle d'accès (ACL) réseau

| Composant | Description | Configuration requise | Exemple (s) de valeur |
| --- | --- | --- | --- |
| ID ACL réseau | Une liste de contrôle d'accès réseau (ACL) autorise ou refuse le trafic entrant ou sortant au niveau du sous-réseau. | Doit autoriser Amazon EVS à communiquer avec :<br>• Serveurs DNS via TCP/UDP le port 53. | acl-0f62c640e793a38a3 |

| Composant | Description | Configuration requise | Exemple (s) de valeur |
|---|---|---|---|
| | | • Sous-réseau VLAN de gestion de l'hôte via HTTPS et SSH.<br>• Sous-réseau VLAN de la machine virtuelle de gestion via HTTPS et SSH. | |

Enregistrements DNS pour les composants VCF

| Composant | Description | Configuration requise | Exemple d'adresse IP | Exemple de nom d'hôte |
|---|---|---|---|---|
| Hôte ESX 1 | Adresse IP et nom d'hôte définis dans l'enregistrement A et l'enregistrement PTR pour l'hôte ESX 1. | Amazon EVS nécessite une zone de recherche directe DNS avec des enregistrements A et une zone de recherche inversée avec des enregistrements PTR créés pour chaque hôte ESX dans chaque déploiement EVS. | 10.1.0.10 | esxi01 |
| Hôte ESX 2 | Adresse IP et nom d'hôte définis dans | Amazon EVS nécessite une zone de | 10.1.0.11 | esxi02 |

| Composant | Description | Configuration requise | Exemple d'adresse IP | Exemple de nom d'hôte |
|---|---|---|---|---|
| | l'enregistrement A et l'enregistrement PTR pour l'hôte ESX 2. | recherche directe DNS avec des enregistrements A et une zone de recherche inversée avec des enregistrements PTR créés pour chaque hôte ESX dans chaque déploiement EVS. | | |
| Hôte ESX 3 | Adresse IP et nom d'hôte définis dans l'enregistrement A et l'enregistrement PTR pour l'hôte ESX 3. | Amazon EVS nécessite une zone de recherche directe DNS avec des enregistrements A et une zone de recherche inversée avec des enregistrements PTR créés pour chaque hôte ESX dans chaque déploiement EVS. | 10.1.0.12 | esxi03 |

| Composant | Description | Configuration requise | Exemple d'adresse IP | Exemple de nom d'hôte |
|---|---|---|---|---|
| Hôte ESX 4 | Adresse IP et nom d'hôte définis dans l'enregistrement A et l'enregistrement PTR pour l'hôte ESX 4. | Amazon EVS nécessite une zone de recherche directe DNS avec des enregistrements A et une zone de recherche inversée avec des enregistrements PTR créés pour chaque hôte ESX dans chaque déploiement EVS. | 10.1.0.13 | esxi04 |

| Composant | Description | Configuration requise | Exemple d'adresse IP | Exemple de nom d'hôte |
|---|---|---|---|---|
| dispositif vCenter Server | Adresse IP et nom d'hôte définis dans l'enregistrement A et l'enregistrement PTR du dispositif vCenter Server. | Amazon EVS nécessite une zone de recherche directe DNS avec des enregistrements A et une zone de recherche inversée avec des enregistrements PTR créés pour chaque appliance de gestion VCF dans chaque déploiement EVS. | 10.1.5,10 | vc01 |

| Composant | Description | Configuration requise | Exemple d'adresse IP | Exemple de nom d'hôte |
|---|---|---|---|---|
| Cluster NSX Manager | Adresse IP et nom d'hôte définis dans l'enregistrement A et l'enregistrement PTR du cluster NSX Manager. | Amazon EVS nécessite une zone de recherche directe DNS avec des enregistrements A et une zone de recherche inversée avec des enregistrements PTR créés pour chaque appliance de gestion VCF dans chaque déploiement EVS. | 10.1.5,11 | nsx |

| Composant | Description | Configuration requise | Exemple d'adresse IP | Exemple de nom d'hôte |
|---|---|---|---|---|
| Appareil SDDC Manager | Adresse IP et nom d'hôte définis dans l'enregistrement A et l'enregistrement PTR de l'appliance SDDC Manager. | Amazon EVS nécessite une zone de recherche directe DNS avec des enregistrements A et une zone de recherche inversée avec des enregistrements PTR créés pour chaque appliance de gestion VCF dans chaque déploiement EVS. | 10.1.5,12 | sddcm01 |

| Composant | Description | Configuration requise | Exemple d'adresse IP | Exemple de nom d'hôte |
|---|---|---|---|---|
| Appliance Cloud Builder | Adresse IP et nom d'hôte définis dans l'enregistrement A et l'enregistrement PTR de l'appliance Cloud Builder. | Amazon EVS nécessite une zone de recherche directe DNS avec des enregistrements A et une zone de recherche inversée avec des enregistrements PTR créés pour chaque appliance de gestion VCF dans chaque déploiement EVS. | 10.1.5,13 | cb01 |

| Composant | Description | Configuration requise | Exemple d'adresse IP | Exemple de nom d'hôte |
|---|---|---|---|---|
| dispositif NSX Edge 1 | Adresse IP et nom d'hôte définis dans l'enregistrement A et l'enregistrement PTR du dispositif NSX Edge 1. | Amazon EVS nécessite une zone de recherche directe DNS avec des enregistrements A et une zone de recherche inversée avec des enregistrements PTR créés pour chaque appliance de gestion VCF dans chaque déploiement EVS. | 10.1.5,14 | arête 01 |

| Composant | Description | Configuration requise | Exemple d'adresse IP | Exemple de nom d'hôte |
|---|---|---|---|---|
| dispositif NSX Edge 2 | Adresse IP et nom d'hôte définis dans l'enregistrement A et l'enregistrement PTR du dispositif NSX Edge 2. | Amazon EVS nécessite une zone de recherche directe DNS avec des enregistrements A et une zone de recherche inversée avec des enregistrements PTR créés pour chaque appliance de gestion VCF dans chaque déploiement EVS. | 10.1.5,15 | edge02 |

| Composant | Description | Configuration requise | Exemple d'adresse IP | Exemple de nom d'hôte |
|---|---|---|---|---|
| dispositif NSX Manager 1 | Adresse IP et nom d'hôte définis dans l'enregistrement A et l'enregistrement PTR du dispositif NSX Manager 1. | Amazon EVS nécessite une zone de recherche directe DNS avec des enregistrements A et une zone de recherche inversée avec des enregistrements PTR créés pour chaque appliance de gestion VCF dans chaque déploiement EVS. | 10.1.5,16 | nsx01 |

| Composant | Description | Configuration requise | Exemple d'adresse IP | Exemple de nom d'hôte |
|---|---|---|---|---|
| dispositif NSX Manager 2 | Adresse IP et nom d'hôte définis dans l'enregistrement A et l'enregistrement PTR du dispositif NSX Manager 2. | Amazon EVS nécessite une zone de recherche directe DNS avec des enregistrements A et une zone de recherche inversée avec des enregistrements PTR créés pour chaque appliance de gestion VCF dans chaque déploiement EVS. | 10.1.5,17 | nsx02 |

| Composant | Description | Configuration requise | Exemple d'adresse IP | Exemple de nom d'hôte |
|---|---|---|---|---|
| dispositif NSX Manager 3 | Adresse IP et nom d'hôte définis dans l'enregistrement A et l'enregistrement PTR du dispositif NSX Manager 3. | Amazon EVS nécessite une zone de recherche directe DNS avec des enregistrements A et une zone de recherche inversée avec des enregistrements PTR créés pour chaque appliance de gestion VCF dans chaque déploiement EVS. | 10.1.5,18 | nsx03 |

Infrastructure de serveur de routage VPC

| Composant | Description | Configuration requise | Exemple (s) de valeur |
|---|---|---|---|
| ID du serveur de routage | Amazon EVS utilise Amazon VPC Route Server pour activer le routage dynamique basé sur le BGP vers votre réseau sous-jacent VPC. | Vous devez spécifier un serveur de routage qui partage des itinéraires vers au moins deux points de terminaison du serveur de routage dans le sous-réseau d'accès au service. | rs-0a1b2c3d4e5f67890 |

| Composant | Description | Configuration requise | Exemple (s) de valeur |
| --- | --- | --- | --- |
| | | L'ASN homologue configuré sur le serveur de routage et l'homologue NSX Edge doivent correspondre, et les adresses IP des homologues doivent être uniques. | |
| association de serveurs de routes | Connexion entre un serveur de routage et un VPC. | Votre serveur de routage doit être associé à votre VPC. | <pre>{<br>    "RouteServerAssociation": {<br>        "RouteServerId": "rs-0a1b2c3d4e5f67890",<br>        "VpcId": "vpc-1",<br>        "State": "associating"<br>    }<br>}</pre> |

| Composant | Description | Configuration requise | Exemple (s) de valeur |
| --- | --- | --- | --- |
| ASN BGP côté serveur de routage VPC (ASN côté Amazon) | L'ASN côté Amazon représente le AWS côté de la session BGP entre le serveur de routage VPC et l'homologue NSX Edge. Vous spécifiez cet ASN BGP lors de la création du serveur de routage. Pour plus d'informations, consultez la section Créer un serveur de routage dans le guide de l'utilisateur Amazon VPC. | Cette valeur doit être unique et comprise entre 1 et 4294967295. AWS recommande d'utiliser un ASN privé compris entre 64512 et 65534 (ASN 16 bits) ou 4200000000-4294967294 (ASN 32 bits). | 65001 |
| ID du point de terminaison 1 du serveur de route | Un point de terminaison de serveur de route est un composant AWS géré au sein d'un sous-réseau qui facilite les connexions BGP (Border Gateway Protocol) entre votre serveur de route et vos homologues BGP. | Vous devez déployer le point de terminaison du serveur de routage dans le sous-réseau d'accès au service. | rse-0123456789abcdef0 |

| Composant | Description | Configuration requise | Exemple (s) de valeur |
|---|---|---|---|
| ID du serveur de route homologue 1 | L'homologue du serveur de route est une session d'appairage BGP entre un point de terminaison du serveur de route et le périphérique déployé dans AWS (NSX Edge). | La valeur ASN homologue spécifiée dans l'homologue du serveur de routage doit correspondre à la valeur ASN homologue utilisée pour la passerelle NSX Edge de niveau 0. | rsp-0123456789abcdef0 |
| adresse IP du serveur de routage homologue 1 (côté EVS NSX Edge 1) | Adresse IP de l'homologue du serveur de route (`PeerAddress` ). | Doit utiliser une adresse IP unique non utilisée provenant du VLAN de liaison ascendante NSX. Amazon EVS appliquera cette adresse IP à NSX Edge 1 dans le cadre du déploiement et établira un accord avec le point de terminaison du serveur de routage. | 10.1.7.10 |
| adresse ENI du point de terminaison homologue 1 du serveur de route | Adresse IP ENI du point de terminaison de l'homologue du serveur de route (`EndpointEniAddress` ). | Généré automatiquement par le serveur de route lors de la création du pair. | 10.1.7.11 |

| Composant | Description | Configuration requise | Exemple (s) de valeur |
| --- | --- | --- | --- |
| ID du point de terminaison 2 du serveur de route | Un point de terminaison de serveur de route est un composant AWS géré au sein d'un sous-réseau qui facilite les connexions BGP (Border Gateway Protocol) entre votre serveur de route et vos homologues BGP. | Vous devez déployer le point de terminaison du serveur de routage dans le sous-réseau d'accès au service. | rse-fedcba9876543210f |
| ID homologue 2 du serveur de routage (côté EVS NSX Edge 2) | L'homologue du serveur de route est une session d'appairage BGP entre un point de terminaison du serveur de route et le périphérique déployé dans AWS (NSX Edge). | La valeur ASN homologue spécifiée dans l'homologue du serveur de routage doit correspondre à la valeur ASN homologue utilisée pour la passerelle NSX Edge de niveau 0. | rsp-fedcba9876543210f |

| Composant | Description | Configuration requise | Exemple (s) de valeur |
| --- | --- | --- | --- |
| adresse IP du serveur de routage homologue 2 | Adresse IP de l'homologue du serveur de route (`PeerAddress` ). | Doit utiliser une adresse IP unique provenant du VLAN de liaison ascendant e NSX. Amazon EVS appliquera cette adresse IP à NSX Edge 2 dans le cadre du déploieme nt et établira un accord avec le point de terminaison du serveur de routage. | 10.1.7.200 |
| adresse ENI du point de terminais on homologue 2 du serveur de route | Adresse IP ENI du point de terminais on de l'homolog ue du serveur de route (`EndpointE niAddress` ). | Généré automatiq uement par le serveur de route lors de la création du pair. | 10.1.7.201 |

| Composant | Description | Configuration requise | Exemple (s) de valeur |
| --- | --- | --- | --- |
| propagation du serveur de routage | La propagation du serveur de routage installe les routes du FIB sur la table de routage que vous avez spécifiée. | Vous devez spécifier la table de routage associée à votre sous-réseau d'accès aux services. Amazon EVS prend uniquement en charge la IPv4 mise en réseau pour le moment. | { "RouteServerEndpoint": { "RouteServerId": "rs-1", "RouteServerEndpointId": "rse-1", "VpcId": "vpc-1", "SubnetId": "subnet-1", "State": "pending" } } |
| BGP ASN du côté homologue de NSX | BGP ASN pour le côté NSX de la connexion. | Suggérer l'utilisation de l'ASN 65000 par défaut de NSX | 65000 |

Ressources d'accès à Internet HCX (facultatif)

| Composant | Description | Configuration requise | Exemple (s) de valeur |
| --- | --- | --- | --- |
| IDENTIFIANT IPAM | Amazon VPC IP Address Manager (IPAM) est utilisé pour gérer les adresses IP pour l'accès Internet HCX. | Doit être configuré pour fournir des IPv4 adresses publiques. Nécessaire uniquement pour la configuration de l'accès Internet HCX. | ipam-0123456789abcdef0 |
| ID du pool IPAM | Un pool IPv4 IPAM public appartenant à Amazon qui fournit | Doit être configuré en tant que IPv4 pool public. Nécessaire uniquement pour | ipam-pool-0123456789abcdef0 |

| Composant | Description | Configuration requise | Exemple (s) de valeur |
|---|---|---|---|
| | des adresses pour les composants HCX. | la configuration de l'accès Internet HCX. | |
| Bloc CIDR VLAN public HCX | Bloc IPv4 CIDR public secondaire alloué depuis le pool IPAM pour le sous-réseau VLAN public HCX. | Doit avoir un masque réseau /28 et être alloué à partir du pool public IPAM appartenant à Amazon. Nécessaire uniquement pour la configuration de l'accès Internet HCX. | 18,97,137,0/28 |
| Adresses IP élastiques | Adresses IP élastiques séquentielles allouées à partir du pool IPAM pour les composants HCX. | Au moins 3 EIPs provenant du même pool IPAM pour HCX Manager, HCX Interconnect Appliance (HCX-IX) et HCX Network Extension (HCX-NE). Nécessaire uniquement pour la configuration de l'accès Internet HCX. | eipalloc-0123456789abcdef0, eipalloc-0123456789abcdef1, eipalloc-0123456789abcdef2 |

# Commencer à utiliser Amazon Elastic VMware Service

Utilisez ce guide pour démarrer avec Amazon Elastic VMware Service (Amazon EVS). Vous allez apprendre à créer un environnement Amazon EVS avec des hôtes au sein de votre propre Amazon Virtual Private Cloud (VPC).

Une fois que vous aurez terminé, vous disposerez d'un environnement Amazon EVS que vous pourrez utiliser pour migrer vos charges de travail VMware basées sur vSphere vers le. AWS Cloud

> **Important**
>
> Pour démarrer le plus simplement et le plus rapidement possible, cette rubrique inclut les étapes de création d'un VPC et spécifie les exigences minimales pour la configuration du serveur DNS et la création de l'environnement Amazon EVS. Avant de créer ces ressources, nous vous recommandons de planifier votre espace d'adressage IP et la configuration de votre enregistrement DNS en fonction de vos besoins. Vous devez également vous familiariser avec les exigences de VCF 5.2.x. Consultez les notes de mise à jour de VCF 5.2.x pour obtenir des informations de version pertinentes.

> **Important**
>
> Pour plus d'informations sur les versions VCF fournies par Amazon EVS, consultez. the section called “Versions et EC2 instances VCF”

Rubriques

- Créez une ACL réseau pour contrôler le trafic du sous-réseau Amazon EVS VLAN
- Création d'un environnement Amazon EVS
- Vérifier la création de l'environnement Amazon EVS
- Associez explicitement des sous-réseaux VLAN Amazon EVS à une table de routage VPC
- Récupérez les informations d'identification VCF et accédez aux appareils de gestion VCF
- Nettoyage
- Étapes suivantes

## Conditions préalables

Avant de commencer, vous devez effectuer les tâches prérequises pour Amazon EVS. Pour de plus amples informations, veuillez consulter Configuration d'Amazon Elastic VMware Service.

## Création d'un VPC avec des sous-réseaux et des tables de routage

> **Note**
>
> Le VPC, les sous-réseaux et l'environnement Amazon EVS doivent tous être créés dans le même compte. Amazon EVS ne prend pas en charge le partage entre comptes de sous-réseaux VPC ou d'environnements Amazon EVS.

Example

Amazon VPC console

1. Ouvrez la Amazon VPC console.
2. Sur le tableau de bord VPC, choisissez Create VPC (Créer un VPC).
3. Sous Ressources à créer, choisissez VPC et plus encore.
4. Maintenez l'option Génération automatique de balise de nom sélectionnée pour créer des balises de nom pour les ressources VPC, ou désactivez-la pour fournir vos propres balises de nom pour les ressources VPC.
5. Pour le bloc IPv4 CIDR, entrez un bloc IPv4 CIDR. Un VPC doit disposer d'un bloc IPv4 CIDR. Assurez-vous de créer un VPC suffisamment dimensionné pour accueillir les sous-

réseaux Amazon EVS. Pour de plus amples informations, veuillez consulter the section called "Considérations relatives au réseau Amazon EVS".

> **Note**
>
> Amazon EVS n'est pas compatible pour le IPv6 moment.

6. Conservez la location en tant que`Default`. Lorsque cette option est sélectionnée, les EC2 instances lancées dans ce VPC utiliseront l'attribut de location spécifié lors du lancement des instances. Amazon EVS lance des EC2 instances bare metal en votre nom.
7. Pour Nombre de zones de disponibilité (AZs), choisissez 1.

> **Note**
>
> Amazon EVS prend uniquement en charge les déploiements mono-AZ pour le moment.

8. Développez Personnaliser AZs et choisissez l'AZ pour vos sous-réseaux.

> **Note**
>
> Vous devez effectuer le déploiement dans une AWS région où Amazon EVS est pris en charge. Pour plus d'informations sur la disponibilité de la région Amazon EVS, consultez la section Points de terminaison et quotas Amazon Elastic VMware Service dans le Guide de référence AWS général.

9. (Facultatif) Si vous avez besoin d'une connexion Internet, dans Nombre de sous-réseaux publics, choisissez 1.
10. Pour Nombre de sous-réseaux privés, choisissez 1. Ce sous-réseau privé sera utilisé comme sous-réseau d'accès au service que vous avez fourni à Amazon EVS lors de l'étape de création de l'environnement. Pour de plus amples informations, veuillez consulter the section called "Sous-réseau d'accès au service".
11. Pour choisir les plages d'adresses IP pour vos sous-réseaux, développez Personnaliser les blocs CIDR des sous-réseaux.

> **Note**
>
> Les sous-réseaux VLAN Amazon EVS devront également être créés à partir de cet espace CIDR VPC. Assurez-vous de laisser suffisamment d'espace dans le bloc

d'adresse CIDR VPC pour les sous-réseaux VLAN requis par le service. Pour de plus amples informations, consultez the section called "Considérations relatives au réseau Amazon EVS".

12. (Facultatif) Pour accorder l'accès IPv4 à Internet aux ressources, pour les passerelles NAT, choisissez In 1 AZ. Notez que des coûts sont associés aux passerelles NAT. Pour plus d'informations, consultez la section Tarification des passerelles NAT.

> **Note**
>
> Amazon EVS nécessite l'utilisation d'une passerelle NAT pour permettre la connectivité Internet sortante.

13. Pour VPC endpoints (Points de terminaison d'un VPC), choisissez None (Aucun).

> **Note**
>
> Amazon EVS ne prend pas en charge les points de terminaison VPC de passerelle Amazon S3 pour le moment. Pour activer la Amazon S3 connectivité, vous devez configurer un point de terminaison VPC d'interface à l'aide AWS PrivateLink de for. Amazon S3Pour plus d'informations, consultez AWS PrivateLink le guide Amazon S3 de l'utilisateur d'Amazon Simple Storage Service.

14. Pour les options DNS, conservez les valeurs par défaut sélectionnées. Amazon EVS exige que votre VPC dispose d'une capacité de résolution DNS pour tous les composants VCF.
15. (Facultatif) Pour ajouter une balise à votre VPC, développez Balises supplémentaires, choisissez Ajouter une nouvelle balise et saisissez une clé et une valeur de balise.
16. Sélectionnez Create VPC (Créer un VPC).

> **Note**
>
> Lors de la création d'un VPC, crée Amazon VPC automatiquement une table de routage principale et y associe implicitement des sous-réseaux par défaut.

AWS CLI

1. Ouvrez une session de terminal.

2. Créez un VPC avec un sous-réseau privé et un sous-réseau public facultatif dans une seule zone de disponibilité.

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

   VPC_ID=$ (aws ec2 describe-vpcs \ --filters Name=tag:name, values=EVS-VPC \ --query 'Vpcs [0]. VpcId'\ --texte de sortie) ---

3. Activez les noms d'hôte DNS et le support 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. Créez un sous-réseau privé dans le 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. Stockez l'ID de sous-réseau privé à utiliser dans les commandes suivantes.

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

6. (Facultatif) Créez un sous-réseau public si vous avez besoin d'une connexion 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. (Facultatif) Stockez l'ID de sous-réseau public à utiliser dans les commandes suivantes.

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

8. (Facultatif) Créez et attachez une passerelle Internet si le sous-réseau public est créé.

```
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. (Facultatif) Créez une passerelle NAT si vous avez besoin d'une connexion 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. Créez et configurez les tables de routage nécessaires.

```
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. Ajoutez les itinéraires nécessaires aux tables de routage.

```
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. Associez les tables de routage à vos sous-réseaux.

```
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**
>
> Lors de la création d'un VPC, crée Amazon VPC automatiquement une table de routage principale et y associe implicitement des sous-réseaux par défaut.

# Choisissez votre option de connectivité HCX

Sélectionnez une option de connectivité pour votre environnement Amazon EVS :

- Connectivité privée : fournit des voies réseau hautes performances pour HCX, optimisant ainsi la fiabilité et la cohérence. Nécessite l'utilisation de AWS Direct Connect ou d' Site-to-Siteun VPN pour la connectivité réseau externe.
- Connectivité Internet : utilise l'Internet public pour établir une voie de migration flexible et rapide à configurer. Nécessite l'utilisation du gestionnaire d'adresses IP VPC (IPAM) et d'adresses IP élastiques.

Pour une analyse détaillée, voirthe section called “Options de connectivité HCX”.

Choisissez votre option :

- Option A : Connectivité privée uniquement → Continuer versthe section called “Configuration de la table de routage principale du VPC”.
- Option B : Connexion Internet → Continuer versthe section called “Configuration de la connectivité Internet HCX”.

## Configuration de la connectivité Internet HCX

> **Note**
>
> Ignorez cette section si vous avez choisi la connectivité privée HCX et passez àthe section called “Configuration de la table de routage principale du VPC”.

Pour activer la connectivité Internet HCX pour Amazon EVS, vous devez :

- Assurez-vous que le quota de votre gestionnaire d'adresses IP VPC (IPAM) pour la longueur du masque réseau de blocs IPv4 CIDR public contigu fourni par Amazon est de /28 ou plus.

  > **Important**
  >
  > L'utilisation de tout bloc IPv4 CIDR public contigu fourni par Amazon avec une longueur de masque réseau inférieure à /28 entraînera des problèmes de connectivité HCX. Pour plus d'informations sur l'augmentation des quotas IPAM, consultez la section Quotas pour votre IPAM.

- Créez un pool IPAM et un pool IPv4 IPAM public avec un CIDR dont la longueur de masque réseau minimale est de /28.
- Allouez au moins deux adresses IP élastiques (EIPs) depuis le pool IPAM pour les appliances HCX Manager et HCX Interconnect (HCX-IX). Allouez une adresse IP élastique supplémentaire pour chaque appliance réseau HCX que vous devez déployer.
- Ajoutez le bloc d'adresse IPv4 CIDR public en tant que CIDR supplémentaire à votre VPC.

Pour plus d'informations sur la gestion de la connectivité Internet HCX après la création de l'environnement, consultezthe section called “Connectivité publique HCX”.

Création d'un IPAM

Suivez ces étapes pour créer un IPAM.

> **Note**
>
> Vous pouvez utiliser le niveau gratuit d'IPAM pour créer des ressources IPAM à utiliser avec Amazon EVS. Bien que l'IPAM lui-même soit gratuit avec le niveau gratuit, vous êtes responsable des coûts des autres AWS services utilisés conjointement avec l'IPAM, tels que les passerelles NAT et les IPv4 adresses publiques que vous utilisez au-delà de la limite du niveau gratuit. Pour plus d'informations sur la tarification de l'IPAM, consultez la page de Amazon VPC tarification.

> **Note**
>
> Amazon EVS ne prend pas en charge l'adresse IPv6 globale unicast (GUA) privée pour le CIDRs moment.

### Création d'un pool IPv4 IPAM public

Suivez ces étapes pour créer un IPv4 pool public.

IPAM console

1. Ouvrez la console IPAM.
2. Dans le panneau de navigation, choisissez Pools (Groupes).
3. Choisissez la portée Public. Pour plus d'informations sur les scopes, voir Fonctionnement de l'IPAM.
4. Sélectionnez Create pool (Créer un groupe).
5. (Facultatif) Ajoutez une valeur Name tag (Étiquette de nom) du groupe et une Description du groupe.
6. Sous Famille d'adresses, sélectionnez IPv4.
7. Sous Planification des ressources, laissez sélectionné Planifier l'espace IP dans la portée.
8. Sous Paramètres régionaux, choisissez les paramètres régionaux du groupe. Le paramètre régional est la AWS région dans laquelle vous souhaitez que ce pool IPAM soit disponible pour les allocations. Les paramètres régionaux que vous choisissez doivent correspondre à la AWS région dans laquelle votre VPC est déployé.
9. Sous Service, sélectionnez EC2 (EIP/VPC). Cela annoncera les CIDRs allocations provenant de ce pool pour le EC2 service Amazon (pour les adresses IP élastiques).
10. Sous Source IP publique, sélectionnez appartenant à Amazon.
11. Sous CIDRs Provisionner, sélectionnez Ajouter un CIDR public appartenant à Amazon.
12. Sous Masque réseau, choisissez une longueur de masque réseau CIDR. /28 est la longueur de masque réseau minimale requise.
13. Sélectionnez Create pool (Créer un groupe).

AWS CLI

1. Ouvrez une session de terminal.
2. Obtenez l'identifiant de portée publique auprès de votre IPAM.

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

3. Créez un pool IPAM dans le périmètre public.

```
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. Stockez l'ID du pool à utiliser dans les commandes suivantes.

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

5. Provisionnez un bloc CIDR à partir du pool avec une longueur de masque réseau minimale de /28.

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

### Allouer des adresses IP élastiques à partir du pool IPAM

Procédez comme suit pour allouer des adresses IP élastiques (EIPs) à partir du pool IPAM pour les appliances HCX Service Mesh.

Amazon VPC console

1. Ouvrez la console VPC Amazon.
2. Dans le volet de navigation, sélectionnez Elastic IPs.
3. Choisissez Allocate Elastic IP address (Allouer l'adresse IP Elastic).
4. Sélectionnez Allouer à l'aide d'un pool IPv4 IPAM.
5. Sélectionnez le IPv4 pool public appartenant à Amazon que vous avez précédemment configuré.
6. Sous Allouer la méthode IPAM, choisissez Saisir manuellement l'adresse dans le pool IPAM.

> **Important**
>
> Vous ne pouvez pas associer les deux premiers EIPs ou le dernier EIP du bloc CIDR IPAM public au sous-réseau VLAN. Elles EIPs sont réservées en tant qu'adresses réseau, passerelle par défaut et adresses de diffusion. Amazon EVS génère une erreur de validation si vous tentez de les EIPs associer au sous-réseau VLAN.

> **Important**
>
> Entrez manuellement les adresses dans le pool IPAM pour vous assurer EIPs que les réserves Amazon EVS ne sont pas allouées. Si vous autorisez IPAM à choisir l'EIP, IPAM peut allouer un EIP réservé par Amazon EVS, ce qui provoquera un échec lors de l'association de l'EIP au sous-réseau VLAN.

7. Spécifiez l'EIP à allouer à partir du pool IPAM.
8. Choisissez Allouer.
9. Répétez cette procédure pour allouer le reste EIPs dont vous avez besoin. Vous devez en allouer au moins deux EIPs depuis le pool IPAM pour les appliances HCX Manager et HCX Interconnect (HCX-IX). Allouez un EIP supplémentaire pour chaque appliance réseau HCX que vous devez déployer.

AWS CLI

1. Ouvrez une session de terminal.
2. Obtenez l'ID du pool IPAM que vous avez créé précédemment.

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

3. Allouez des adresses IP élastiques à partir du pool IPAM. Vous devez en allouer au moins deux EIPs depuis le pool IPAM pour les appliances HCX Manager et HCX Interconnect (HCX-IX). Allouez un EIP supplémentaire pour chaque appliance réseau HCX que vous devez déployer.

> **Important**
>
> Vous ne pouvez pas associer les deux premiers EIPs ou le dernier EIP du bloc CIDR IPAM public à un sous-réseau VLAN. Elles EIPs sont réservées en tant qu'adresses réseau, passerelle par défaut et adresses de diffusion. Amazon EVS génère une erreur de validation si vous tentez de les EIPs associer au sous-réseau VLAN.

> **Important**
>
> Entrez manuellement les adresses dans le pool IPAM pour vous assurer EIPs que les réserves Amazon EVS ne sont pas allouées. Si vous autorisez IPAM à choisir l'EIP, IPAM peut allouer un EIP réservé par Amazon EVS, ce qui provoquera un échec lors de l'association de l'EIP au sous-réseau 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
```

Ajoutez le bloc IPv4 CIDR public du pool IPAM au VPC pour la connectivité Internet HCX

Pour activer la connectivité Internet HCX, vous devez ajouter le bloc d'adresse IPv4 CIDR public du pool IPAM à votre VPC en tant que CIDR supplémentaire. Amazon EVS utilise ce bloc CIDR pour connecter VMware HCX à votre réseau. Suivez ces étapes pour ajouter le bloc CIDR à votre VPC.

**Important**

Vous devez saisir manuellement le bloc IPv4 CIDR que vous ajoutez à votre VPC. Amazon EVS ne prend pas en charge l'utilisation d'un bloc CIDR alloué par iPam pour le moment. L'utilisation d'un bloc CIDR alloué par IPAM peut entraîner l'échec de l'association EIP.

Amazon VPC console

1. Ouvrez la console VPC Amazon.
2. Dans le volet de navigation, sélectionnez Votre VPCs.
3. Sélectionnez le VPC que vous avez créé précédemment, puis choisissez Actions, Modifier. CIDRs
4. Choisissez Ajouter un nouveau IPV4 CIDR.
5. Sélectionnez la saisie manuelle IPV4 CIDR.
6. Spécifiez le bloc CIDR du pool IPAM public que vous avez créé précédemment.

AWS CLI

1. Ouvrez une session de terminal.
2. Obtenez l'ID du pool IPAM et le bloc CIDR provisionné.

```
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. Ajoutez le bloc CIDR à votre VPC.

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

## Configuration de la table de routage principale du VPC

Les sous-réseaux VLAN Amazon EVS sont implicitement associés à la table de routage principale du VPC. Pour permettre la connectivité aux services dépendants tels que le DNS ou les systèmes sur site afin de réussir le déploiement de l'environnement, vous devez configurer la table de routage principale pour autoriser le trafic vers ces systèmes. La table de routage principale doit inclure une route pour le CIDR du VPC. L'utilisation de la table de routage principale n'est requise que pour le déploiement initial de l'environnement Amazon EVS. Après le déploiement de l'environnement, vous pouvez configurer votre environnement pour utiliser une table de routage personnalisée. Pour de plus amples informations, veuillez consulter the section called “Configurer une table de routage personnalisée”.

Après le déploiement de l'environnement, vous devez associer explicitement chacun des sous-réseaux Amazon EVS VLAN à une table de routage dans votre VPC. La connectivité NSX échoue si vos sous-réseaux VLAN ne sont pas explicitement associés à une table de routage VPC. Nous vous recommandons vivement d'associer explicitement vos sous-réseaux à une table de routage personnalisée après le déploiement de l'environnement. Pour de plus amples informations, veuillez consulter the section called “Configuration de la table de routage principale du VPC”.

> **Important**
>
> Amazon EVS prend en charge l'utilisation d'une table de routage personnalisée uniquement après la création de l'environnement Amazon EVS. Les tables de routage personnalisées ne

doivent pas être utilisées lors de la création de l'environnement Amazon EVS, car cela peut entraîner des problèmes de connectivité.

# Configuration des serveurs DNS et NTP à l'aide du jeu d'options DHCP du VPC

**Important**

Le déploiement de votre environnement échoue si vous ne répondez pas aux exigences Amazon EVS suivantes :

- Incluez une adresse IP de serveur DNS principal et une adresse IP de serveur DNS secondaire dans le jeu d'options DHCP.
- Incluez une zone de recherche directe DNS avec des enregistrements A pour chaque appliance de gestion VCF et hôte Amazon EVS de votre déploiement.
- Incluez une zone de recherche inversée DNS avec des enregistrements PTR pour chaque appliance de gestion VCF et hôte Amazon EVS de votre déploiement.
- Configurez la table de routage principale du VPC pour vous assurer qu'il existe une route vers vos serveurs DNS.
- Assurez-vous que l'enregistrement de votre nom de domaine est valide et n'a pas expiré, et qu'il n'existe pas de nom d'hôte ou d'adresse IP en double.
- Configurez vos groupes de sécurité et vos listes de contrôle d'accès réseau (ACLs) pour permettre à Amazon EVS de communiquer avec :
  - Serveurs DNS via TCP/UDP le port 53.
  - Sous-réseau VLAN de gestion de l'hôte via HTTPS et SSH.
  - Sous-réseau VLAN de gestion via HTTPS et SSH.

Amazon EVS utilise le jeu d'options DHCP de votre VPC pour récupérer les éléments suivants :

- Serveurs DNS (Domain Name System) pour la résolution des adresses IP de l'hôte.
- Noms de domaine pour la résolution DNS.
- Serveurs NTP (Network Time Protocol) pour la synchronisation de l'heure.

Vous pouvez créer un ensemble d'options DHCP à l'aide de la Amazon VPC console ou AWS CLI. Pour plus d'informations, voir Création d'un ensemble d'options DHCP dans le guide de l' Amazon VPC utilisateur.

## Configuration des serveurs DNS

La configuration DNS permet la résolution du nom d'hôte dans votre environnement Amazon EVS. Pour déployer correctement un environnement Amazon EVS, le jeu d'options DHCP de votre VPC doit comporter les paramètres DNS suivants :

- Adresse IP du serveur DNS principal et adresse IP du serveur DNS secondaire dans le jeu d'options DHCP.
- Une zone de recherche directe DNS avec des enregistrements A pour chaque appliance de gestion VCF et hôte Amazon EVS de votre déploiement.
- Une zone de recherche inversée avec des enregistrements PTR pour chaque appliance de gestion VCF et hôte Amazon EVS de votre déploiement. Pour la configuration NTP, vous pouvez utiliser l'adresse `169.254.169.123` NTP Amazon par défaut ou une autre IPv4 adresse que vous préférez.

Pour plus d'informations sur la configuration des serveurs DNS dans un jeu d'options DHCP, voir Création d'un jeu d'options DHCP.

### Configuration du DNS pour une connectivité sur site

Pour la connectivité sur site, nous recommandons d'utiliser les zones hébergées privées Route 53 avec des résolveurs entrants. Cette configuration permet une résolution DNS hybride, dans laquelle vous pouvez utiliser Route 53 pour le DNS interne au sein de votre VPC et l'intégrer à votre infrastructure DNS sur site existante. Cela permet aux ressources de votre VPC de résoudre les noms de domaine hébergés sur votre réseau local, et vice versa, sans nécessiter de configurations complexes. Si nécessaire, vous pouvez également utiliser votre propre serveur DNS avec les résolveurs sortants Route 53. Pour connaître les étapes de configuration, consultez les sections Création d'une zone hébergée privée et Transfert de requêtes DNS entrantes vers votre VPC dans le guide du développeur Amazon Route 53.

> **Note**
>
> L'utilisation à la fois de Route 53 et d'un serveur DNS (Domain Name System) personnalisé dans le jeu d'options DHCP peut provoquer un comportement inattendu.

> **Note**
>
> Si vous utilisez des noms de domaine DNS personnalisés définis dans une zone hébergée privée dans Route 53, ou si vous utilisez un DNS privé avec des points de terminaison VPC d'interface (AWS PrivateLink), vous devez définir les attributs `enableDnsHostnames` et `enableDnsSupport` sur. `true` Pour plus d'informations, consultez la section Attributs DNS de votre VPC.

### Résoudre les problèmes d'accessibilité du DNS

Amazon EVS nécessite une connexion permanente au gestionnaire SDDC et aux serveurs DNS dans le cadre de l'option DHCP définie par votre VPC pour accéder aux enregistrements DNS. Si la connexion permanente à SDDC Manager devient indisponible, Amazon EVS ne sera plus en mesure de valider l'état de l'environnement et vous risquez de perdre l'accès à l'environnement. Pour connaître les étapes à suivre pour résoudre ce problème, consultezthe section called “Le contrôle d'accessibilité a échoué”.

## Configuration des serveurs NTP

Les serveurs NTP fournissent le temps à votre réseau. Une référence temporelle cohérente et précise sur votre EC2 instance Amazon est essentielle pour de nombreuses tâches et processus liés à l'environnement VCF. La synchronisation de l'heure est essentielle pour :

- Journalisation et audit du système
- Opérations de sécurité
- Gestion du système distribué
- Résolution des problèmes

Vous pouvez saisir les IPv4 adresses d'un maximum de quatre serveurs NTP dans le jeu d'options DHCP de votre VPC. Vous pouvez spécifier le service Amazon Time Sync à l' IPv4

adresse`169.254.169.123`. Par défaut, les EC2 instances Amazon déployées par Amazon EVS utilisent le service Amazon Time Sync à l' IPv4 adresse. `169.254.169.123`

Pour plus d'informations sur les serveurs NTP, consultez la RFC 2123. Pour plus d'informations sur Amazon Time Sync Service, consultez les sections Synchronisation précise de l'horloge et de l'heure dans votre EC2 instance et Configurer le NTP sur les hôtes VMware Cloud Foundation dans la documentation VMware Cloud Foundation.

Pour configurer les paramètres NTP

1. Choisissez votre source NTP :
   - Amazon Time Sync Service (recommandé)
   - Serveurs NTP personnalisés
2. Ajoutez des serveurs NTP à votre ensemble d'options DHCP. Pour plus d'informations, consultez la section Créer un ensemble d'options DHCP dans le guide de l'utilisateur Amazon VPC.
3. Vérifiez la synchronisation de l'heure. Pour plus d'informations sur la configuration du jeu d'options DHCP, consultezthe section called “Configurez le jeu d'options DHCP de votre VPC”.

Configuration de la connectivité réseau sur site (facultatif)

Vous pouvez configurer la connectivité entre votre centre de données sur site et votre AWS infrastructure à l'aide Direct Connect d'une passerelle de transit associée ou d'une AWS Site-to-Site connexion VPN à une passerelle de transit.

Pour permettre la connectivité aux systèmes sur site afin de réussir le déploiement de l'environnement, vous devez configurer la table de routage principale du VPC pour autoriser le trafic vers ces systèmes. Pour de plus amples informations, veuillez consulter the section called “Configuration de la table de routage principale du VPC”.

Une fois l'environnement Amazon EVS créé, vous devez mettre à jour les tables de routage de la passerelle de transit avec le CIDRs VPC créé dans l'environnement Amazon EVS. Pour de plus amples informations, veuillez consulter the section called “Configurer les tables de routage des passerelles de transit et les préfixes Direct Connect pour la connectivité sur site (facultatif)”.

Pour plus d'informations sur la configuration d'une Direct Connect connexion, consultez la section Passerelles et associations de Direct Connect passerelles de transit. Pour plus d'informations sur l'utilisation d' AWS Site-to-Site un VPN avec AWS Transit Gateway, consultez la section Pièces

jointes AWS Site-to-Site VPN dans Amazon VPC Transit Gateways dans le guide de l'utilisateur de Amazon VPC Transit Gateway.

> **Note**
>
> Amazon EVS ne prend pas en charge la connectivité via une interface virtuelle privée (VIF) AWS Direct Connect ou via une connexion AWS Site-to-Site VPN qui aboutit directement au VPC sous-jacent.

## Configuration d'une instance de serveur de routage VPC avec des points de terminaison et des homologues

Amazon EVS utilise Amazon VPC Route Server pour activer le routage dynamique basé sur le BGP vers votre réseau sous-jacent VPC. Vous devez spécifier un serveur de routage qui partage des itinéraires vers au moins deux points de terminaison du serveur de routage dans le sous-réseau d'accès au service. L'ASN pair configuré sur les pairs du serveur de routage doit correspondre et les adresses IP des pairs doivent être uniques.

Si vous configurez le serveur de route pour la connectivité Internet HCX, vous devez configurer les propagations du serveur de route pour le sous-réseau d'accès au service et le sous-réseau public que vous avez créés lors de la première étape de cette procédure.

> **Important**
>
> Le déploiement de votre environnement échoue si vous ne répondez pas aux exigences Amazon EVS suivantes pour la configuration du serveur de routage VPC :
>
> - Vous devez configurer au moins deux points de terminaison du serveur de routage dans le sous-réseau d'accès au service.
> - Lors de la configuration du protocole BGP (Border Gateway Protocol) pour la passerelle de niveau 0, la valeur ASN du pair du serveur de routage VPC doit correspondre à la valeur ASN du pair NSX Edge.
> - Lorsque vous créez les deux homologues du serveur de routage, vous devez utiliser une adresse IP unique provenant du VLAN de liaison montante NSX pour chaque point de terminaison. Ces deux adresses IP seront attribuées aux NSX Edge lors du déploiement de l'environnement Amazon EVS.

- Lorsque vous activez la propagation par le serveur de routage, vous devez vous assurer que toutes les tables de routage propagées possèdent au moins une association de sous-réseau explicite. La publicité de route BGP échoue si les tables de routage propagées n'ont pas d'association de sous-réseau explicite.

Pour plus d'informations sur la configuration du serveur de routage VPC, consultez le didacticiel de démarrage du serveur de routage.

**Important**

Lorsque vous activez la propagation par le serveur de routage, assurez-vous que toutes les tables de routage propagées possèdent au moins une association de sous-réseau explicite. La publicité de route BGP échoue si la table de routage possède une association de sous-réseau explicite.

**Note**

Pour la détection de la réactivité entre pairs du serveur Route, Amazon EVS prend uniquement en charge le mécanisme BGP keepalive par défaut. Amazon EVS ne prend pas en charge la détection du transfert bidirectionnel (BFD) à sauts multiples.

**Note**

Nous vous recommandons d'activer les itinéraires persistants pour l'instance du serveur de routage avec une durée de persistance comprise entre 1 et 5 minutes. Si cette option est activée, les itinéraires seront conservés dans la base de données de routage du serveur de routage même si toutes les sessions BGP se terminent. Pour plus d'informations, voir Création d'un serveur de routage dans le guide de Amazon VPC l'utilisateur.

> **Note**
>
> Si vous utilisez une passerelle NAT ou une passerelle de transit, assurez-vous que votre serveur de routage est correctement configuré pour propager les routes NSX vers les tables de routage VPC.

### Résolution des problèmes

Si vous rencontrez des problèmes :

- Vérifiez que chaque table de routage possède une association de sous-réseau explicite.
- Vérifiez que les valeurs ASN homologues saisies pour le serveur de route et la passerelle NSX Tier-0 correspondent.
- Vérifiez que les adresses IP des points de terminaison du serveur de route sont uniques.
- Vérifiez l'état de propagation des itinéraires dans vos tables de routage.
- Utilisez la journalisation par les pairs du serveur de routage VPC pour surveiller l'état de la session BGP et résoudre les problèmes de connexion. Pour plus d'informations, consultez la section Connexion par les pairs au serveur Route dans le guide de l'utilisateur Amazon VPC.

## Créez une ACL réseau pour contrôler le trafic du sous-réseau Amazon EVS VLAN

Amazon EVS utilise une liste de contrôle d'accès réseau (ACL) pour contrôler le trafic à destination et en provenance des sous-réseaux VLAN Amazon EVS. Vous pouvez utiliser l'ACL réseau par défaut pour votre VPC, ou vous pouvez créer une ACL réseau personnalisée pour votre VPC avec des règles similaires à celles de vos groupes de sécurité afin d'ajouter une couche de sécurité à votre VPC. Pour plus d'informations, consultez la section Créer une ACL réseau pour votre VPC dans le guide de l'utilisateur Amazon VPC.

Si vous envisagez de configurer la connectivité Internet HCX, assurez-vous que les règles ACL réseau que vous configurez autorisent les connexions entrantes et sortantes nécessaires pour les composants HCX. Pour plus d'informations sur les exigences relatives aux ports HCX, consultez le guide de l'utilisateur VMware HCX.

**Important**

Si vous vous connectez via Internet, l'association d'une adresse IP élastique à un VLAN fournit un accès Internet direct à toutes les ressources de ce sous-réseau VLAN. Assurez-vous que les listes de contrôle d'accès réseau appropriées sont configurées pour restreindre l'accès en fonction de vos exigences de sécurité.

**Important**

EC2 les groupes de sécurité ne fonctionnent pas sur les interfaces réseau élastiques associées aux sous-réseaux Amazon EVS VLAN. Pour contrôler le trafic à destination et en provenance des sous-réseaux VLAN Amazon EVS, vous devez utiliser une liste de contrôle d'accès réseau.

# Création d'un environnement Amazon EVS

**Important**

Pour démarrer le plus simplement et le plus rapidement possible, cette rubrique décrit les étapes à suivre pour créer un environnement Amazon EVS avec des paramètres par défaut. Avant de créer un environnement, nous vous recommandons de vous familiariser avec tous les paramètres et de déployer un environnement répondant à vos besoins. Les environnements ne peuvent être configurés que lors de la création initiale de l'environnement. Les environnements ne peuvent pas être modifiés une fois que vous les avez créés. Pour un aperçu de tous les paramètres d'environnement Amazon EVS possibles, consultez le guide de référence de l'API Amazon EVS.

**Note**

Votre identifiant d'environnement sera mis à la disposition d'Amazon EVS dans toutes les AWS régions pour répondre aux besoins de conformité des licences VCF.

> **Note**
>
> Les environnements Amazon EVS doivent être déployés dans la même région et la même zone de disponibilité que les sous-réseaux VPC et VPC.

Effectuez cette étape pour créer un environnement Amazon EVS avec des hôtes et des sous-réseaux VLAN.

Example

Amazon EVS console

1. Accédez à la console Amazon EVS.

   > **Note**
   >
   > Assurez-vous que la AWS région affichée dans le coin supérieur droit de votre console est celle dans laquelle vous souhaitez créer votre environnement. AWS Si ce n'est pas le cas, choisissez le menu déroulant à côté du nom de la AWS région et choisissez la AWS région que vous souhaitez utiliser.

2. Dans le panneau de navigation, choisissez Environments (Environnements).
3. Choisissez Create environment.
4. Sur la page de validation des exigences d'Amazon EVS, vérifiez que les exigences de service sont satisfaites. Pour de plus amples informations, veuillez consulter Configuration d'Amazon Elastic VMware Service.
   a. (Facultatif) Dans Nom, entrez un nom d'environnement.
   b. Pour la version Environment, choisissez votre version VCF. Pour plus d'informations sur les versions VCF fournies par Amazon EVS, consultez. the section called “Versions et EC2 instances VCF”
   c. Dans le champ Site ID, entrez votre ID de site Broadcom.
   d. Pour la clé de solution VCF, entrez une clé de solution VCF (VMware vSphere 8 Enterprise Plus pour VCF). Cette clé de licence ne peut pas être utilisée par un environnement existant.

> **Note**
>
> La clé de solution VCF doit comporter au moins 256 cœurs.

> **Note**
>
> Votre licence VCF sera mise à la disposition d'Amazon EVS dans toutes les AWS régions pour garantir la conformité des licences. Amazon EVS ne valide pas les clés de licence. Pour valider les clés de licence, consultez le support de Broadcom.

> **Note**
>
> Amazon EVS exige que vous conserviez une clé de solution VCF valide dans SDDC Manager pour que le service fonctionne correctement. Si vous gérez la clé de solution VCF à l'aide de vSphere Client après le déploiement, vous devez vous assurer que les clés apparaissent également dans l'écran de licence de l'interface utilisateur de SDDC Manager.

e. Pour la clé de licence vSAN, entrez une clé de licence vSAN. Cette clé de licence ne peut pas être utilisée par un environnement existant.

> **Note**
>
> La clé de licence vSAN doit avoir au moins 110 TiB de capacité vSAN.

> **Note**
>
> Votre licence VCF sera mise à la disposition d'Amazon EVS dans toutes les AWS régions pour garantir la conformité des licences. Amazon EVS ne valide pas les clés de licence. Pour valider les clés de licence, consultez le support de Broadcom.

> **Note**
>
> Amazon EVS exige que vous conserviez une clé de licence vSAN valide dans SDDC Manager pour choisir le service qui fonctionnera correctement. Si vous gérez la clé de licence vSAN à l'aide de vSphere Client après le déploiement, vous devez vous assurer que les clés apparaissent également dans l'écran de licence de l'interface utilisateur de SDDC Manager.

f. Pour connaître les termes des licences VCF, cochez la case pour confirmer que vous avez acheté et que vous continuerez à maintenir le nombre requis de licences logicielles VCF pour couvrir tous les cœurs de processeur physiques de l'environnement Amazon EVS. Les informations relatives à votre logiciel VCF dans Amazon EVS seront partagées avec Broadcom afin de vérifier la conformité des licences.

g. Choisissez Suivant.

5. Sur la page Spécifier les détails de l'hôte, effectuez les étapes suivantes quatre fois pour ajouter quatre hôtes à l'environnement. Les environnements Amazon EVS nécessitent quatre hôtes pour le déploiement initial.

   a. Choisissez Ajouter les détails de l'hôte.

   b. Pour le nom d'hôte DNS, entrez le nom d'hôte de l'hôte.

   c. Pour le type d'instance, choisissez le type d' EC2 instance.

   d. Pour la version hôte ESX, lors de la création de l'environnement, une version ESX par défaut sera utilisée pour la version VCF choisie. Pour plus d'informations, consultez the section called "Versions et EC2 instances VCF".

   > **Important**
   >
   > N'arrêtez pas ou ne mettez pas hors EC2 service les instances déployées par Amazon EVS. Cette action entraîne une perte de données.

   > **Note**
   >
   > Amazon EVS ne prend en charge que les EC2 instances i4i.metal pour le moment.

   e. Pour la paire de clés SSH, choisissez une paire de clés SSH pour l'accès SSH à l'hôte.

f. Choisissez Ajouter un hôte.

6. Sur la page Configurer les réseaux et la connectivité, procédez comme suit.

a. Pour les exigences de connectivité HCX, indiquez si vous souhaitez utiliser HCX avec une connectivité privée ou via Internet.

b. Pour VPC, choisissez le VPC que vous avez créé précédemment.

c. (Pour la connexion Internet HCX uniquement) Pour l'ACL réseau HCX, choisissez à quelle ACL réseau votre VLAN HCX sera associé.

> **Important**
>
> Nous vous recommandons vivement de créer un ACL réseau personnalisé dédié au VLAN HCX. Pour de plus amples informations, veuillez consulter the section called "Configurer le réseau ACL".

d. Pour le sous-réseau d'accès au service, choisissez le sous-réseau privé créé lors de la création du VPC.

e. Pour le groupe de sécurité (facultatif), vous pouvez choisir jusqu'à deux groupes de sécurité qui contrôlent la communication entre le plan de contrôle Amazon EVS et le VPC. Amazon EVS utilise le groupe de sécurité par défaut si aucun groupe de sécurité n'est choisi.

> **Note**
>
> Assurez-vous que les groupes de sécurité que vous choisissez fournissent une connectivité à vos serveurs DNS et aux sous-réseaux Amazon EVS VLAN.

f. Sous Connectivité de gestion, entrez les blocs CIDR à utiliser pour les sous-réseaux Amazon EVS VLAN. Pour le bloc CIDR VLAN à liaison montante HCX, si vous configurez un VLAN HCX public, vous devez spécifier un bloc CIDR avec une longueur de masque réseau exactement de /28. Amazon EVS génère une erreur de validation si une autre taille de bloc CIDR est spécifiée pour le VLAN HCX public. Pour un VLAN HCX privé et tous les autres blocs VLANs CIDR, la longueur minimale du masque réseau que vous pouvez utiliser est /28 et la longueur maximale est /24.

> **Important**
>
> Les sous-réseaux VLAN Amazon EVS ne peuvent être créés que lors de la création de l'environnement Amazon EVS et ne peuvent pas être modifiés une fois

l'environnement créé. Vous devez vous assurer que les blocs CIDR du sous-réseau VLAN sont correctement dimensionnés avant de créer l'environnement. Vous ne pourrez pas ajouter de sous-réseaux VLAN une fois l'environnement déployé. Pour de plus amples informations, veuillez consulter the section called “Considérations relatives au réseau Amazon EVS”.

g. Sous Expansion VLANs, entrez les blocs CIDR pour les sous-réseaux Amazon EVS VLAN supplémentaires qui peuvent être utilisés pour étendre les fonctionnalités VCF au sein d'Amazon EVS, par exemple en activant NSX Federation.

h. Sous Connectivité workload/VCF, entrez le bloc CIDR pour le VLAN de liaison montante NSX et choisissez deux homologues du serveur de routage VPC IDs qui correspondent aux points de terminaison du serveur de routage via la liaison montante NSX.

> **Note**
>
> Amazon EVS nécessite une instance de serveur de route VPC associée à deux points de terminaison du serveur de route et à deux homologues du serveur de route avant le déploiement d'EVS. Cette configuration permet un routage dynamique basé sur le protocole BGP via la liaison montante NSX. Pour de plus amples informations, veuillez consulter the section called “Configuration d'une instance de serveur de routage VPC avec des points de terminaison et des homologues”.

i. Choisissez Suivant.

7. Sur la page Spécifier les noms d'hôte DNS de gestion, procédez comme suit.

a. Sous Noms d'hôte DNS du dispositif de gestion, entrez les noms d'hôte DNS des machines virtuelles devant héberger les dispositifs de gestion VCF. Si vous utilisez Route 53 comme fournisseur DNS, choisissez également la zone hébergée qui contient vos enregistrements DNS.

b. Sous Credentials, indiquez si vous souhaitez utiliser la clé KMS AWS gérée pour Secrets Manager ou une clé KMS gérée par le client que vous avez fournie. Cette clé est utilisée pour chiffrer les informations d'identification VCF requises pour utiliser les dispositifs SDDC Manager, NSX Manager et vCenter.

> **Note**
>
> Des coûts d'utilisation sont associés aux clés KMS gérées par le client. Pour plus d'informations, consultez la page de tarification de AWS KMS.

c. Choisissez Suivant.

8. (Facultatif) Sur la page Ajouter des balises, ajoutez les balises que vous souhaitez attribuer à cet environnement et choisissez Next.

> **Note**
>
> Les hôtes créés dans le cadre de cet environnement recevront la balise suivante :`DoNotDelete-EVS-<environmentid>-<hostname>`.

> **Note**
>
> Les balises associées à l'environnement Amazon EVS ne se propagent pas aux AWS ressources sous-jacentes telles que EC2 les instances. Vous pouvez créer des balises sur les AWS ressources sous-jacentes à l'aide de la console de service correspondante ou du AWS CLI.

9. Sur la page Réviser et créer, passez en revue votre configuration et choisissez Create environment.

> **Important**
>
> Lors du déploiement de l'environnement, Amazon EVS crée les sous-réseaux VLAN EVS et les associe implicitement à la table de routage principale. Une fois le déploiement terminé, vous devez associer explicitement les sous-réseaux Amazon EVS VLAN à une table de routage à des fins de connectivité NSX. Pour de plus amples informations, veuillez consulter the section called “Associez explicitement des sous-réseaux VLAN Amazon EVS à une table de routage VPC”.

> **Note**
>
> Amazon EVS déploie une version groupée récente de VMware Cloud Foundation qui peut ne pas inclure de mises à jour de produit individuelles, connues sous le nom de correctifs asynchrones. Une fois ce déploiement terminé, nous vous recommandons vivement de passer en revue et de mettre à jour les produits individuels à l'aide de l'outil Async Patch Tool (AP Tool) de Broadcom ou de l'automatisation LCM intégrée au produit SDDC Manager. Les mises à niveau de NSX doivent être effectuées en dehors de SDDC Manager.

> **Note**
>
> La création d'un environnement peut prendre plusieurs heures.

AWS CLI

1. Ouvrez une session de terminal.
2. Créez un environnement Amazon EVS. Vous trouverez ci-dessous un exemple de `aws evs create-environment` demande.

> **Important**
>
> Avant d'exécuter la `aws evs create-environment` commande, vérifiez que toutes les conditions requises pour Amazon EVS sont remplies. Le déploiement de l'environnement échoue si les conditions préalables ne sont pas remplies. Pour de plus amples informations, veuillez consulter Configuration d'Amazon Elastic VMware Service.

> **Important**
>
> Lors du déploiement de l'environnement, Amazon EVS crée les sous-réseaux VLAN EVS et les associe implicitement à la table de routage principale. Une fois le déploiement terminé, vous devez associer explicitement les sous-réseaux Amazon

EVS VLAN à une table de routage à des fins de connectivité NSX. Pour de plus amples informations, veuillez consulter the section called "Associez explicitement des sous-réseaux VLAN Amazon EVS à une table de routage VPC".

> **Note**
>
> Amazon EVS déploie une version groupée récente de VMware Cloud Foundation qui peut ne pas inclure de mises à jour de produit individuelles, connues sous le nom de correctifs asynchrones. Une fois ce déploiement terminé, nous vous recommandons vivement de passer en revue et de mettre à jour les produits individuels à l'aide de l'outil Async Patch Tool (AP Tool) de Broadcom ou de l'automatisation LCM intégrée au produit SDDC Manager. Les mises à niveau de NSX doivent être effectuées en dehors de SDDC Manager.

> **Note**
>
> Le déploiement de l'environnement peut prendre plusieurs heures.

- Pour `--vpc-id`, spécifiez le VPC que vous avez créé précédemment avec une plage d'adresse IPv4 CIDR minimale de /22.
- Pour `--service-access-subnet-id`, spécifiez l'ID unique du sous-réseau privé créé lors de la création du VPC.
- Pour `--vcf-version`, voir the section called "Versions et EC2 instances VCF" pour les versions VCF fournies par Amazon EVS,
- Avec `--terms-accepted`, vous confirmez que vous avez acheté et que vous continuerez à maintenir le nombre requis de licences logicielles VCF pour couvrir tous les cœurs de processeur physiques de l'environnement Amazon EVS. Les informations relatives à votre logiciel VCF dans Amazon EVS seront partagées avec Broadcom afin de vérifier la conformité des licences.
- Pour `--license-info`, entrez votre clé de solution VCF (VMware vSphere 8 Enterprise Plus pour VCF) et votre clé de licence vSAN.

> **Note**
>
> La clé de solution VCF doit comporter au moins 256 cœurs. La clé de licence vSAN doit avoir au moins 110 TiB de capacité vSAN.

> **Note**
>
> Amazon EVS exige que vous conserviez une clé de solution VCF et une clé de licence vSAN valides dans SDDC Manager pour que le service fonctionne correctement. Si vous gérez ces clés de licence à l'aide de vSphere Client après le déploiement, vous devez vous assurer qu'elles apparaissent également dans l'écran de licence de l'interface utilisateur de SDDC Manager.

> **Note**
>
> La clé de solution VCF et la clé de licence vSAN ne peuvent pas être utilisées par un environnement Amazon EVS existant.

- Pour `--initial-vlans` spécifier les plages d'adresses CIDR pour les sous-réseaux VLAN Amazon EVS créés par Amazon EVS en votre nom. Ils VLANs sont utilisés pour déployer des dispositifs de gestion VCF. Si vous configurez un VLAN HCX public, vous devez spécifier un bloc CIDR avec une longueur de masque réseau exactement égale à /28. Amazon EVS génère une erreur de validation si une autre taille de bloc CIDR est spécifiée pour le VLAN HCX public. Pour un VLAN HCX privé et tous les autres blocs VLANs CIDR, la longueur minimale du masque réseau que vous pouvez utiliser est /28 et la longueur maximale est /24.
- `hcxNetworkAclIdest` utilisé lors de la configuration de la connectivité Internet HCX. Spécifiez une ACL réseau personnalisée pour le VLAN HCX public.

> **Important**
>
> Nous vous recommandons vivement de créer un ACL réseau personnalisé dédié au VLAN HCX. Pour de plus amples informations, veuillez consulter the section called "Configurer le réseau ACL".

> **Important**
>
> Les sous-réseaux VLAN Amazon EVS ne peuvent être créés que lors de la création de l'environnement Amazon EVS et ne peuvent pas être modifiés une fois l'environnement créé. Vous devez vous assurer que les blocs CIDR du sous-réseau VLAN sont correctement dimensionnés avant de créer l'environnement. Vous ne pourrez pas ajouter de sous-réseaux VLAN une fois l'environnement déployé. Pour de plus amples informations, veuillez consulter the section called "Considérations relatives au réseau Amazon EVS".

- Pour `--hosts`, spécifiez les détails des hôtes dont Amazon EVS a besoin pour le déploiement de l'environnement. Incluez le nom d'hôte DNS, le nom de la clé EC2 SSH et le type d' EC2 instance pour chaque hôte. L'ID d'hôte dédié est facultatif.

> **Important**
>
> N'arrêtez pas ou ne mettez pas hors EC2 service les instances déployées par Amazon EVS. Cette action entraîne une perte de données.

> **Note**
>
> Amazon EVS ne prend en charge que les EC2 instances i4i.metal pour le moment.

- Pour `--connectivity-info`, spécifiez l'homologue du serveur de routage à 2 VPC IDs que vous avez créé à l'étape précédente.

> **Note**
>
> Amazon EVS nécessite une instance de serveur de route VPC associée à deux points de terminaison du serveur de route et à deux homologues du serveur de route avant le déploiement d'EVS. Cette configuration permet un routage dynamique basé sur le protocole BGP via la liaison montante NSX. Pour de plus amples informations, veuillez consulter the section called "Configuration d'une instance de serveur de routage VPC avec des points de terminaison et des homologues".

- Pour`--vcf-hostnames`, entrez les noms d'hôte DNS des machines virtuelles qui hébergeront les dispositifs de gestion VCF.
- Pour`--site-id`, entrez votre identifiant de site Broadcom unique. Cet ID permet d'accéder au portail Broadcom, et vous est fourni par Broadcom à la fin de votre contrat logiciel ou à son renouvellement.
- (Facultatif) Pour`--region`, entrez la région dans laquelle votre environnement sera déployé. Si la région n'est pas spécifiée, votre région par défaut est utilisée.

```
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
```

Voici un exemple de réponse.

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

# Vérifier la création de l'environnement Amazon EVS

Example

Amazon EVS console

1. Accédez à la console Amazon EVS.
2. Dans le panneau de navigation, choisissez Environments (Environnements).
3. Sélectionnez l'environnement.
4. Sélectionnez l'onglet Détails.
5. Vérifiez que le statut de l'environnement est passé et que l'état de l'environnement est créé. Cela vous permet de savoir que l'environnement est prêt à être utilisé.

> **Note**
>
> La création d'un environnement peut prendre plusieurs heures. Si l'état de l'environnement indique toujours Création, actualisez la page.

AWS CLI

1. Ouvrez une session de terminal.
2. Exécutez la commande suivante en utilisant l'ID d'environnement de votre environnement et le nom de la région qui contient vos ressources. L'environnement est prêt à être utilisé lorsqu'il l'`environmentState`est`CREATED`.

> **Note**
>
> La création d'un environnement peut prendre plusieurs heures. Si le résultat `environmentState` est toujours affiché`CREATING`, réexécutez la commande pour actualiser le résultat.

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

Voici un exemple de réponse.

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

# Associez explicitement des sous-réseaux VLAN Amazon EVS à une table de routage VPC

Associez explicitement chacun des sous-réseaux Amazon EVS VLAN à une table de routage dans votre VPC. Cette table de routage est utilisée pour permettre aux AWS ressources de communiquer avec des machines virtuelles sur des segments de réseau NSX exécutés avec Amazon EVS. Si vous avez créé un VLAN HCX public, veillez à associer explicitement le sous-réseau VLAN HCX public à une table de routage publique de votre VPC qui achemine vers une passerelle Internet.

Example

Amazon VPC console

1. Accédez à la console VPC.
2. Dans le volet de navigation, choisissez Route tables (Tables de routage).
3. Choisissez la table de routage que vous souhaitez associer aux sous-réseaux Amazon EVS VLAN.
4. Sélectionnez l'onglet Associations de sous-réseaux.
5. Sous Associations de sous-réseaux explicites, sélectionnez Modifier les associations de sous-réseaux.
6. Sélectionnez tous les sous-réseaux Amazon EVS VLAN.
7. Choisissez Save associations (Enregistrer les associations).

AWS CLI

1. Ouvrez une session de terminal.
2. Identifiez le sous-réseau Amazon EVS VLAN. IDs

```
aws ec2 describe-subnets
```

3. Associez vos sous-réseaux Amazon EVS VLAN à une table de routage dans votre VPC.

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

## Associer EIPs au sous-réseau VLAN public HCX (pour la connectivité Internet HCX)

Suivez ces étapes pour associer l'adresse IP élastique (EIPs) du pool IPAM au VLAN public HCX pour la connectivité Internet HCX. Vous devez en associer au moins deux EIPs pour les appliances HCX Manager et HCX Interconnect (HCX-IX). Associez un EIP supplémentaire à chaque appliance réseau HCX que vous devez déployer. Vous pouvez en avoir jusqu' EIPs à 13 dans le pool IPAM associé au VLAN public HCX.

**Important**

La connectivité Internet publique HCX échoue si vous n'associez pas au moins deux connexions EIPs du pool IPAM à un sous-réseau VLAN public HCX.

**Note**

Amazon EVS prend uniquement en charge l'association EIPs avec le VLAN HCX pour le moment.

**Note**

Vous ne pouvez pas associer les deux premiers EIPs ou le dernier EIP du bloc CIDR IPAM public au sous-réseau VLAN. Elles EIPs sont réservées en tant qu'adresses réseau, passerelle par défaut et adresses de diffusion. Amazon EVS génère une erreur de validation si vous tentez de les EIPs associer au sous-réseau VLAN.

Amazon EVS console

1. Accédez à la console Amazon EVS.
2. Dans le menu de navigation, choisissez Environments.
3. Sélectionnez l'environnement.
4. Dans l'onglet Réseaux et connectivité, sélectionnez le VLAN public HCX.
5. Choisissez Associer EIP au VLAN.
6. Sélectionnez la ou les adresses IP élastiques à associer au VLAN public HCX.
7. Choisissez Associer EIPs.
8. Vérifiez les associations EIP pour confirmer qu'elles EIPs ont été associées au VLAN public HCX.

AWS CLI

1. Pour associer une adresse IP élastique à un VLAN, utilisez l'exemple de `associate-eip-to-vlan` commande.

- `environment-id`- L'ID de votre environnement Amazon EVS.
- `vlan-name`- Le nom du VLAN à associer à l'adresse IP élastique.
- `allocation-id`- L'ID d'allocation de l'adresse IP élastique.

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

La commande renvoie des détails sur le VLAN, y compris la nouvelle association 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"
    }
}
```

Le `eipAssociations` tableau montre la nouvelle association, notamment :

- `associationId`- L'identifiant unique de cette association EIP, utilisé pour la dissociation.
- `allocationId`- L'ID d'allocation de l'adresse IP élastique associée.
- `ipAddress`- L'adresse IP attribuée au VLAN.

2. Répétez l'étape pour en associer d'autres EIPs.

### Configurer les tables de routage des passerelles de transit et les préfixes Direct Connect pour la connectivité sur site (facultatif)

Si vous configurez la connectivité réseau sur site à l'aide Direct Connect d'un AWS Site-to-Site VPN avec une passerelle de transit, vous devez mettre à jour les tables de routage de la passerelle de transit avec le CIDRs VPC créé dans l'environnement Amazon EVS. Pour plus d'informations, consultez les tables de routage des passerelles de transit dans Amazon VPC Transit Gateways.

Si vous utilisez AWS Direct Connect, vous devrez peut-être également mettre à jour vos préfixes Direct Connect pour envoyer et recevoir des itinéraires mis à jour depuis le VPC. Pour plus d'informations, voir Autoriser les interactions avec les préfixes pour les passerelles AWS Direct Connect.

## Récupérez les informations d'identification VCF et accédez aux appareils de gestion VCF

Amazon EVS utilise AWS Secrets Manager pour créer, chiffrer et stocker des secrets gérés dans votre compte. Ces secrets contiennent les informations d'identification VCF nécessaires pour installer et accéder aux dispositifs de gestion VCF tels que vCenter Server, NSX et SDDC Manager, ainsi que le mot de passe racine ESX. Pour plus d'informations sur la récupération de secrets, consultez la section Obtenir des AWS secrets depuis Secrets Manager dans le guide de l'utilisateur de AWS Secrets Manager.

> **Note**
>
> Amazon EVS ne gère pas la rotation de vos secrets. Nous vous recommandons de faire tourner vos secrets régulièrement selon une fenêtre de rotation définie afin que vos secrets ne restent pas en circulation trop longtemps.

Après avoir récupéré vos informations d'identification VCF dans AWS Secrets Manager, vous pouvez les utiliser pour vous connecter à vos dispositifs de gestion VCF. Pour plus d'informations, reportez-vous aux sections Connexion à l'interface utilisateur du gestionnaire SDDC et Comment utiliser et configurer votre client vSphere dans la documentation du produit. VMware

## Configuration de la console EC2 série (facultatif)

Par défaut, Amazon EVS active l'ESX Shell sur les hôtes Amazon EVS récemment déployés. Cette configuration permet d'accéder au port série de l' EC2 instance Amazon via la console EC2 série, que vous pouvez utiliser pour résoudre les problèmes de démarrage, de configuration réseau et autres. La console série ne requiert pas que votre instance possède des capacités de mise en réseau. Avec la console série, vous pouvez entrer des commandes sur une EC2 instance en cours d'exécution comme si votre clavier et votre écran étaient directement connectés au port série de l'instance.

La console EC2 série est accessible à l'aide de la EC2 console ou du AWS CLI. Pour plus d'informations, consultez la section EC2 Serial Console pour les instances dans le guide de EC2 l'utilisateur Amazon.

> **Note**
>
> La console EC2 série est le seul mécanisme pris en charge par Amazon EVS pour accéder à l'interface utilisateur de la console directe (DCUI) afin d'interagir avec un hôte ESX localement.

> **Note**
>
> Amazon EVS désactive le SSH à distance par défaut. Pour plus d'informations sur l'activation de SSH pour accéder à l'ESX Shell distant, consultez Remote ESX Shell Access with SSH dans la documentation du produit VMware vSphere.

### Connect à la console EC2 série

Pour vous connecter à la console EC2 série et utiliser l'outil de dépannage que vous avez choisi, certaines tâches préalables doivent être effectuées. Pour plus d'informations, consultez les sections Conditions requises pour la console EC2 série et Connect to the EC2 Serial Console dans le guide de l' EC2 utilisateur Amazon.

> **Note**
>
> Pour vous connecter à la console EC2 série, l'état de votre EC2 instance doit être`running`. Vous ne pouvez pas vous connecter à la console série si l'instance est à l'`terminated`état

`pending` `stopping``stopped`,`shutting-down`,, ou. Pour plus d'informations sur les modifications de l'état des instances, consultez la section Modification de l'état des EC2 instances Amazon dans le guide de EC2 l'utilisateur Amazon.

Configuration de l'accès à la console EC2 série

Pour configurer l'accès à la console EC2 série, vous ou votre administrateur devez accorder l'accès à la console série au niveau du compte, puis configurer des politiques IAM pour accorder l'accès à vos utilisateurs. Pour les instances Linux, vous devez également configurer un utilisateur basé sur un mot de passe pour chaque instance afin que vos utilisateurs puissent utiliser la console série pour le dépannage. Pour plus d'informations, consultez Configurer l'accès à la console EC2 série dans le guide de EC2 l'utilisateur Amazon.

# Nettoyage

Procédez comme suit pour supprimer les AWS ressources créées.

## Supprimer les hôtes et l'environnement Amazon EVS

Suivez ces étapes pour supprimer les hôtes et l'environnement Amazon EVS. Cette action supprime l'installation VMware VCF qui s'exécute dans votre environnement Amazon EVS.

> **Note**
>
> Pour supprimer un environnement Amazon EVS, vous devez d'abord supprimer tous les hôtes de l'environnement. Un environnement ne peut pas être supprimé si des hôtes y sont associés.

Example

Amazon EVS console

1. Accédez à la console Amazon EVS.
2. Dans le volet de navigation, choisissez Environment.
3. Sélectionnez l'environnement qui contient les hôtes à supprimer.

4. Sélectionnez l'onglet Hosts.
5. Sélectionnez l'hôte et choisissez Supprimer dans l'onglet Hôtes. Répétez cette étape pour chaque hôte de l'environnement.
6. En haut de la page Environnements, choisissez Supprimer, puis Supprimer l'environnement.

> **Note**
>
> La suppression de l'environnement supprime également les sous-réseaux VLAN Amazon EVS et les secrets Secrets Manager AWS créés par Amazon EVS. AWS les ressources que vous créez ne sont pas supprimées. Ces ressources peuvent continuer à entraîner des coûts.

7. Si vous avez des réservations Amazon EC2 Capacity dont vous n'avez plus besoin, assurez-vous de les avoir annulées. Pour plus d'informations, consultez la section Annuler une réservation de capacité dans le guide de EC2 l'utilisateur Amazon.

AWS CLI

1. Ouvrez une session de terminal.
2. Identifiez l'environnement qui contient l'hôte à supprimer.

```
aws evs list-environments
```

Voici un exemple de réponse.

```
{
    "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. Supprimez les hôtes de l'environnement. Vous trouverez ci-dessous un exemple de `aws evs delete-environment-host` demande.

> **Note**
>
> Pour pouvoir supprimer un environnement, vous devez d'abord supprimer tous les hôtes qu'il contient.

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

4. Répétez les étapes précédentes pour supprimer les hôtes restants de votre environnement.
5. Supprimez l'environnement.

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

> **Note**
>
> La suppression de l'environnement supprime également les sous-réseaux VLAN Amazon EVS et les secrets Secrets Manager AWS créés par Amazon EVS. Les autres AWS ressources que vous créez ne sont pas supprimées. Ces ressources peuvent continuer à entraîner des coûts.

6. Si vous avez des réservations Amazon EC2 Capacity dont vous n'avez plus besoin, assurez-vous de les avoir annulées. Pour plus d'informations, consultez la section Annuler une réservation de capacité dans le guide de EC2 l'utilisateur Amazon.

Supprimer les ressources IPAM (pour la connectivité Internet HCX)

Si vous avez configuré la connectivité Internet HCX, suivez ces étapes pour supprimer vos ressources IPAM.

1. Libérez les allocations EIP depuis le pool IPAM public. Pour plus d'informations, consultez la section Publier une allocation dans le guide de l'utilisateur du gestionnaire d'adresses IP VPC.
2. Déprovisionnez le IPv4 CIDR public du pool IPAM. Pour plus d'informations, consultez la section Déprovisionnement CIDRs à partir d'un pool dans le guide de l'utilisateur du gestionnaire d'adresses IP VPC.
3. Supprimez le pool IPAM public. Pour plus d'informations, consultez Supprimer un pool dans le Guide de l'utilisateur du gestionnaire d'adresses IP VPC.
4. Supprimez l'IPAM. Pour plus d'informations, consultez Supprimer un IPAM dans le guide de l'utilisateur du gestionnaire d'adresses IP VPC.

## Supprimer les composants du serveur de routage VPC

Pour savoir comment supprimer les composants du serveur de routage Amazon VPC que vous avez créés, consultez la section Nettoyage du serveur de routage dans le guide de l'utilisateur Amazon VPC.

## Supprimer la liste de contrôle d'accès réseau (ACL)

Pour savoir comment supprimer une liste de contrôle d'accès réseau, consultez Supprimer une liste de contrôle d'accès réseau pour votre VPC dans le guide de l'utilisateur Amazon VPC.

## Dissocier et supprimer les tables de routage des sous-réseaux

Pour savoir comment dissocier et supprimer les tables de routage de sous-réseaux, consultez la section Tables de routage de sous-réseaux dans le guide de l'utilisateur Amazon VPC.

## Suppression des sous-réseaux

Supprimez les sous-réseaux VPC, y compris le sous-réseau d'accès aux services. Pour savoir comment supprimer des sous-réseaux VPC, consultez Supprimer un sous-réseau dans le guide de l'utilisateur Amazon VPC.

> **Note**
>
> Si vous utilisez Route 53 pour le DNS, supprimez les points de terminaison entrants avant de tenter de supprimer le sous-réseau d'accès au service. Dans le cas contraire, vous ne pourrez pas supprimer le sous-réseau d'accès au service.

> **Note**
>
> Amazon EVS supprime les sous-réseaux VLAN en votre nom lorsque l'environnement est supprimé. Les sous-réseaux VLAN Amazon EVS ne peuvent être supprimés que lorsque l'environnement est supprimé.

### Suppression du VPC

Pour savoir comment supprimer le VPC, consultez Supprimer votre VPC dans le guide de l'utilisateur Amazon VPC.

## Étapes suivantes

Migrez vos charges de travail vers Amazon EVS à l'aide de VMware Hybrid Cloud Extension (VMware HCX). Pour de plus amples informations, veuillez consulter Migration.

# Migrer les charges de travail vers Amazon EVS à l'aide de HCX VMware

Une fois Amazon EVS déployé, vous pouvez déployer VMware HCX avec une connectivité Internet privée ou publique afin de faciliter la migration des charges de travail vers Amazon EVS. Pour plus d'informations, consultez Getting Started with VMware HCX dans le guide de l'utilisateur de VMware HCX.

> **Important**
>
> La migration HCX via Internet n'est généralement pas recommandée pour :
>
> - Applications sensibles à l'instabilité ou à la latence du réseau.
> - Opérations vMotion critiques.
> - Migrations à grande échelle avec des exigences de performance strictes.
>
> Pour ces scénarios, nous vous recommandons d'utiliser la connectivité privée HCX. Une connexion dédiée privée offre des performances plus fiables que les connexions Internet.

## Options de connectivité HCX

Vous pouvez migrer des charges de travail vers Amazon EVS en utilisant une connectivité privée avec Direct AWS Connect ou une connexion Site-to-Site VPN, ou en utilisant une connectivité publique.

En fonction de votre situation et des options de connectivité, vous pouvez préférer utiliser une connectivité publique ou privée avec HCX. Par exemple, certains sites peuvent disposer d'une connectivité privée offrant une meilleure cohérence des performances, mais un débit inférieur en raison du cryptage VPN ou des vitesses de liaison limitées. De même, il se peut que vous disposiez d'une connectivité Internet publique à haut débit dont les performances varient davantage. Avec Amazon EVS, vous avez le choix d'utiliser l'option de connectivité qui vous convient le mieux.

Le tableau suivant compare les différences entre la connectivité privée et publique HCX.

| Connectivité privée | Connectivité publique |
| --- | --- |
| Présentation | Présentation |
| Utilise uniquement des connexions privées au sein du VPC. Vous pouvez éventuellement utiliser AWS Direct Connect ou un Site-to-Site VPN avec une passerelle de transit pour la connectivité réseau externe. | Utilise une connectivité Internet publique avec des adresses IP élastiques, permettant des migrations sans connexion privée dédiée. |
| Le mieux adapté pour | Le mieux adapté pour |
| • Opérations vMotion sensibles au facteur temps.<br>• Migrations à grande échelle.<br>• Applications sensibles à la latence/à l'instabilité.<br>• Transferts de données à volume élevé.<br>• Organisations disposant déjà d'une connexion AWS directe ou d'un AWS Site-to-Site VPN. | • Emplacements sans connexion AWS AWS Site-to-Site directe/VPN.<br>• Projets sensibles aux coûts. |
| Principaux avantages | Principaux avantages |
| • Connectivité constante à faible latence.<br>• Allocation de bande passante dédiée.<br>• Performances réseau plus fiables.<br>• Le chiffrement HCX par défaut peut être désactivé pour les environnements privés afin d'optimiser les performances.<br>• Aucune gestion publique des adresses IP n'est requise. | • Configuration plus rapide que la connectivité privée.<br>• Rentable pour les petites migrations. |
| Considérations clés | Considérations clés |
| • Configuration initiale plus complexe. | • Performances réseau plus variables. |

| Connectivité privée | Connectivité publique |
| --- | --- |
| • Coûts d'infrastructure initiaux plus élevés.<br>• Échéancier de mise en œuvre plus long<br>• Aucune connexion Internet directe pour aucun composant HCX. | • Des limites de bande passante sont possibles.<br>• Latence supérieure à celle de la connectivité privée.<br>• Chaque composant nécessite une adresse IP élastique dédiée allouée à partir du pool IPAM public.<br>• Les associations EIP permettent une connectivité Internet directe pour chaque composant HCX. |

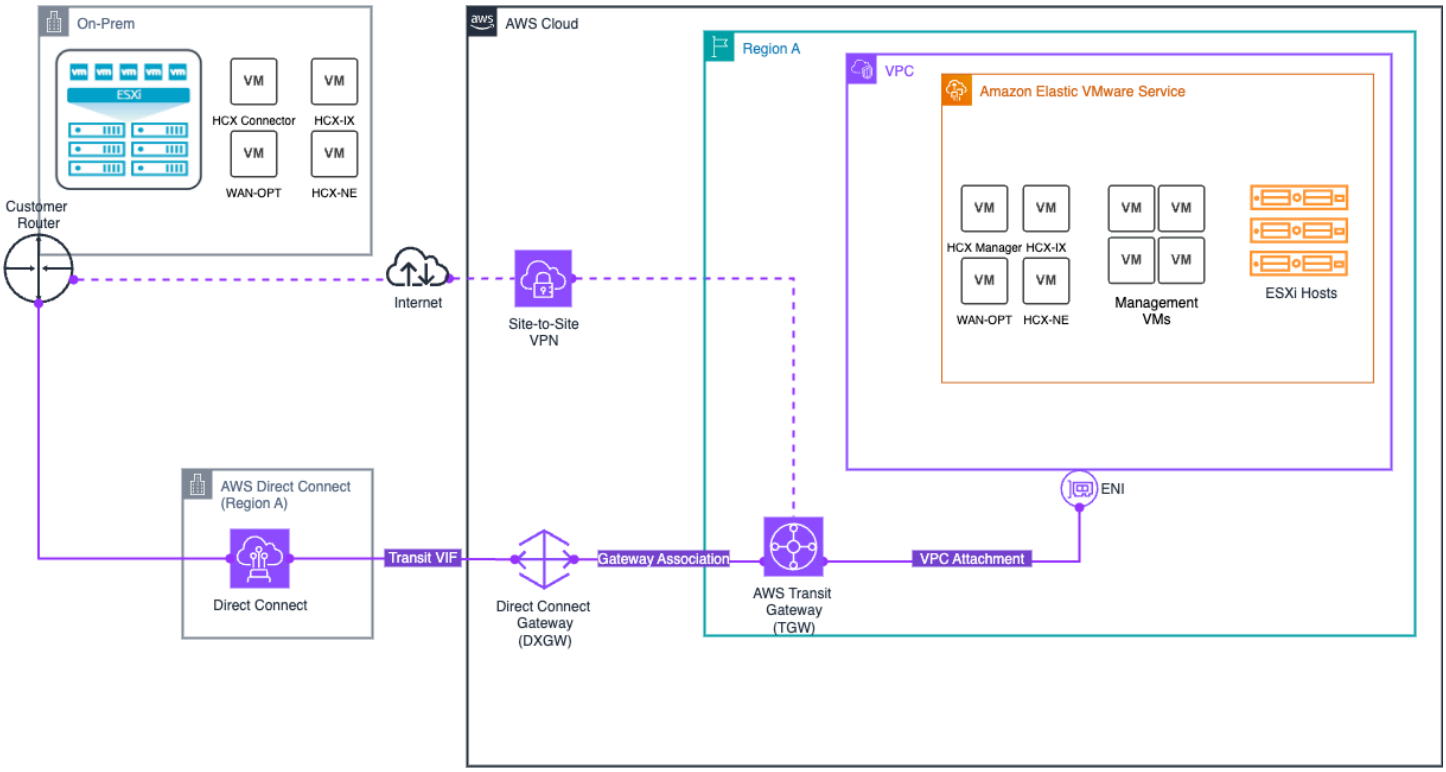
# Architecture de connectivité privée HCX

La solution de connectivité privée HCX intègre plusieurs composants :

- Composants du réseau Amazon EVS
  - Utilise uniquement des sous-réseaux VLAN privés pour des communications sécurisées, y compris un VLAN HCX privé.
  - Supporte le réseau ACLs pour le contrôle du trafic.
  - Prend en charge la propagation BGP dynamique des routes via un serveur de routage VPC privé.
- AWS options de transit réseau gérées pour la connectivité sur site
  - AWS Direct Connect + AWS Transit Gateway vous permet de connecter votre réseau local à Amazon EVS via une connexion dédiée privée. Pour plus d'informations, consultez AWS Direct Connect + AWS Transit Gateway.
  - AWS Site-to-Site VPN + AWS Transit Gateway offre la possibilité de créer une connexion IPsec VPN entre votre réseau distant et la passerelle de transit via Internet. Pour plus d'informations, consultez AWS Transit Gateway + AWS Site-to-Site VPN.

> **Note**
>
> Amazon EVS ne prend pas en charge la connectivité via une interface virtuelle privée (VIF) AWS Direct Connect ou via une connexion AWS Site-to-Site VPN qui aboutit directement au VPC sous-jacent.

Le schéma suivant illustre l'architecture de connectivité privée HCX et montre comment vous pouvez utiliser AWS Direct Connect et le Site-to-Site VPN avec la passerelle de transit pour permettre une migration sécurisée de la charge de travail via une connexion dédiée privée.




# Architecture de connectivité Internet HCX

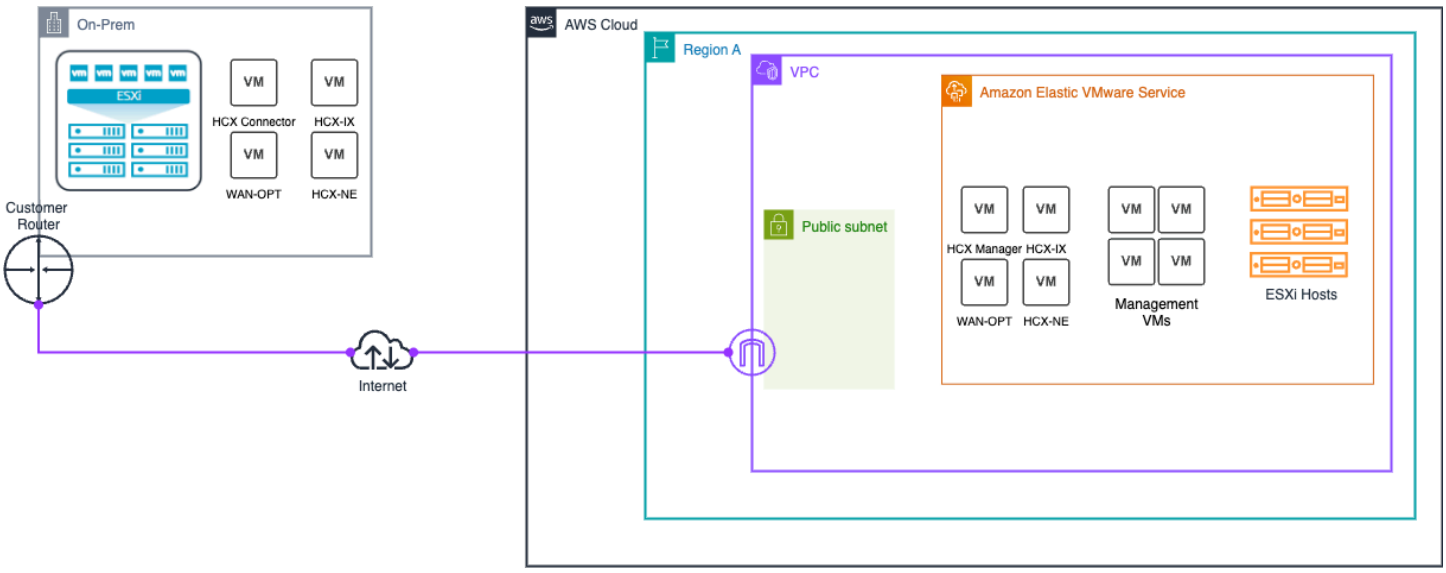
La solution de connectivité Internet HCX est composée de plusieurs composants qui fonctionnent ensemble :

- Composants du réseau Amazon EVS
  - Utilise un sous-réseau VLAN HCX public isolé pour permettre la connectivité Internet entre Amazon EVS et vos appareils HCX sur site.
  - Supporte le réseau ACLs pour le contrôle du trafic.

- Prend en charge la propagation BGP dynamique des routes via un serveur de routage VPC public.
- IPAM et gestion des adresses IP publiques
  - Amazon VPC IP Address Manager (IPAM) gère l'allocation d' IPv4 adresses publiques à partir du pool IPAM public appartenant à Amazon.
  - Le bloc d'adresse CIDR VPC secondaire (/28) est alloué à partir du pool IPAM, créant ainsi un sous-réseau public isolé distinct du CIDR VPC principal.

Pour de plus amples informations, veuillez consulter the section called “Connectivité publique HCX”.

Le schéma suivant illustre l'architecture de connectivité Internet HCX.




# Configuration de la migration HCX

Ce didacticiel explique comment configurer VMware HCX pour migrer vos charges de travail vers Amazon EVS.

## Conditions préalables

Avant d'utiliser VMware HCX avec Amazon EVS, assurez-vous que les conditions requises pour HCX sont remplies. Pour de plus amples informations, veuillez consulter the section called “VMware Prérequis HCX”.

**Important**

Amazon EVS a des exigences uniques en matière de connectivité Internet publique HCX. Si vous avez besoin d'une connectivité publique HCX, vous devez satisfaire aux exigences suivantes :

- Créez un pool IPAM et un pool IPv4 IPAM public avec un CIDR dont la longueur de masque réseau minimale est de /28.
- Allouez au moins deux adresses IP élastiques (EIPs) depuis le pool IPAM pour les appliances HCX Manager et HCX Interconnect (HCX-IX). Allouez une adresse IP élastique supplémentaire pour chaque appliance réseau HCX que vous devez déployer.
- Ajoutez le bloc d'adresse IPv4 CIDR public en tant que CIDR supplémentaire à votre VPC.

Pour de plus amples informations, veuillez consulter the section called “Configuration de la connectivité Internet HCX”.

## Vérifiez l'état du sous-réseau VLAN HCX

Un VLAN est créé pour HCX dans le cadre du déploiement standard d'Amazon EVS. Suivez ces étapes pour vérifier que le sous-réseau VLAN HCX est correctement configuré.

Example

Amazon EVS console

1. Accédez à la console Amazon EVS.
2. Dans le panneau de navigation, choisissez Environments (Environnements).
3. Sélectionnez l'environnement Amazon EVS.
4. Sélectionnez l'onglet Réseaux et connectivité.
5. Sous VLANs, identifiez le VLAN HCX et vérifiez que l'état est créé et que Public est vrai.

AWS CLI

1. Exécutez la commande suivante en utilisant l'ID d'environnement de votre environnement et le nom de la région qui contient vos ressources.

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

2. Dans la sortie de réponse, identifiez le VLAN avec un `functionName` de `hcx` et vérifiez que le `vlanState` est `CREATED` et `isPublic` est défini sur. `true` Voici un exemple de réponse.


```
{
    "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
```

```
        }
    ]
}
```

## Vérifiez que le sous-réseau VLAN HCX est associé à une ACL réseau

Suivez ces étapes pour vérifier que le sous-réseau VLAN HCX est associé à une ACL réseau. Pour plus d'informations sur l'association réseau ACL, consultezthe section called "Créez une ACL réseau pour contrôler le trafic du sous-réseau Amazon EVS VLAN".

> **Important**
>
> Si vous vous connectez via Internet, l'association d'une adresse IP élastique à un VLAN fournit un accès Internet direct à toutes les ressources de ce VLAN. Assurez-vous que les listes de contrôle d'accès réseau appropriées sont configurées pour restreindre l'accès en fonction de vos exigences de sécurité.

> **Important**
>
> EC2 les groupes de sécurité ne fonctionnent pas sur les interfaces réseau élastiques connectées aux sous-réseaux Amazon EVS VLAN. Pour contrôler le trafic à destination et en provenance des sous-réseaux VLAN Amazon EVS, vous devez utiliser une liste de contrôle d'accès réseau (ACL).

Example

Amazon VPC console

1. Accédez à la Amazon VPC console.
2. Dans le volet de navigation, choisissez Network ACLs.
3. Sélectionnez l'ACL réseau à laquelle vos sous-réseaux VLAN sont associés.
4. Sélectionnez l'onglet Associations de sous-réseaux.
5. Vérifiez que le sous-réseau VLAN HCX est répertorié parmi les sous-réseaux associés.

AWS CLI

1. Exécutez la commande suivante en utilisant l'ID de sous-réseau VLAN HCX dans le filtre. `Values`

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

2. Vérifiez que la bonne ACL réseau est renvoyée dans la réponse.

## Vérifiez que les sous-réseaux VLAN EVS sont explicitement associés à une table de routage

Amazon EVS exige que tous les sous-réseaux VLAN EVS soient explicitement associés à une table de routage dans votre VPC. Pour la connectivité Internet HCX, votre sous-réseau VLAN public HCX doit être explicitement associé à une table de routage publique dans votre VPC qui achemine vers une passerelle Internet. Procédez comme suit pour vérifier l'association explicite de la table de routage.

Example

Amazon VPC console

1. Accédez à la console VPC.
2. Dans le volet de navigation, choisissez Route tables (Tables de routage).
3. Choisissez la table de routage à laquelle vos sous-réseaux VLAN EVS doivent être explicitement associés.
4. Sélectionnez l'onglet Associations de sous-réseaux.
5. Sous Associations de sous-réseaux explicites, vérifiez que tous les sous-réseaux VLAN EVS sont répertoriés. Si aucun sous-réseau VLAN n'est répertorié ici, le sous-réseau VLAN est implicitement associé à la table de routage principale. Pour qu'Amazon EVS fonctionne correctement, vous devez associer explicitement tous les sous-réseaux VLAN à une table de routage. Pour le sous-réseau VLAN public HCX, vous devez disposer d'une table de routage publique associée avec une passerelle Internet comme cible. Pour résoudre ce problème, choisissez Modifier les associations de sous-réseaux et ajoutez le ou les sous-réseaux VLAN manquants.

AWS CLI

1. Ouvrez une session de terminal.
2. Exécutez l'exemple de commande suivant pour récupérer des informations sur tous vos sous-réseaux VLAN EVS, y compris l'association de tables de routage. Si aucun sous-réseau VLAN n'est répertorié ici, le sous-réseau VLAN est implicitement associé à la table de routage principale. Pour qu'Amazon EVS fonctionne correctement, vous devez associer explicitement tous les sous-réseaux VLAN à une table de routage. Pour le sous-réseau VLAN public HCX, vous devez disposer d'une table de routage publique associée avec une passerelle Internet comme cible.

   ```
   aws ec2 describe-subnets
   ```

3. Associez explicitement vos sous-réseaux VLAN EVS à une table de routage dans votre VPC. Vous trouverez ci-dessous un exemple de commande.

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

## (Pour la connectivité Internet HCX) Vérifiez qu' EIPs ils sont associés au sous-réseau VLAN HCX

Pour chaque dispositif réseau HCX que vous déployez, vous devez disposer d'un EIP provenant du pool IPAM associé à un sous-réseau VLAN public HCX. Vous devez en associer au moins deux EIPs au sous-réseau VLAN public HCX pour les appliances HCX Manager et HCX Interconnect (HCX-IX). Procédez comme suit pour vérifier que les associations EIP nécessaires existent.

> **Important**
>
> La connectivité Internet publique HCX échoue si vous n'associez pas au moins deux connexions EIPs du pool IPAM à un sous-réseau VLAN public HCX.

> **Note**
>
> Vous ne pouvez pas associer les deux premiers EIPs ou le dernier EIP du bloc CIDR IPAM public à un sous-réseau VLAN. Elles EIPs sont réservées en tant qu'adresses réseau, passerelle par défaut et adresses de diffusion. Amazon EVS génère une erreur de validation si vous tentez de les EIPs associer à un sous-réseau VLAN.

Example

Amazon EVS console

1. Accédez à la console Amazon EVS.
2. Dans le menu de navigation, choisissez Environments.
3. Sélectionnez l'environnement.
4. Sous l'onglet Réseaux et connectivité, sélectionnez le VLAN public HCX.
5. Vérifiez l'onglet Associations EIP pour confirmer qu'elles EIPs ont été associées au VLAN public HCX.

AWS CLI

1. Pour vérifier ceux qui EIPs sont associés au sous-réseau VLAN HCX, utilisez la commande. `list-environment-vlans` Pour`environment-id`, utilisez l'ID unique de l'environnement EVS qui contient le VLAN HCX.

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

   La commande renvoie des informations sur vos associations EIP VLANs, y compris les associations 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"
    },
    ...
  ]
}
```


Le `eipAssociations` tableau montre l'association EIP, notamment :

- `associationId`- L'identifiant unique de cette association EIP.
- `allocationId`- L'ID d'allocation de l'adresse IP élastique associée.
- `ipAddress`- L'adresse IP attribuée au VLAN.

## Créez un groupe de ports distribués avec l'ID VLAN de liaison montante publique HCX

Accédez à l'interface vSphere Client et suivez les étapes décrites dans Ajouter un groupe de ports distribués pour ajouter un groupe de ports distribués à un vSphere Distributed Switch.

Lorsque vous configurez le retour arrière dans l'interface vSphere Client, assurez-vous que uplink1 est un lien montant actif et que uplink2 est un lien montant de secours pour permettre le basculement. Active/Standby Pour le paramètre VLAN dans l'interface vSphere Client, entrez l'ID VLAN HCX que vous avez précédemment identifié.

## (Facultatif) Configurer l'optimisation du réseau WAN HCX

> **Note**
>
> La fonctionnalité d'optimisation WAN n'est plus disponible dans HCX 4.11.3. Pour plus d'informations, consultez les notes de mise à jour de HCX 4.11.3.

Le service d'optimisation WAN HCX (HCX-WO) améliore les caractéristiques de performance des lignes privées ou des chemins Internet en appliquant des techniques d'optimisation WAN telles que la réduction des données et le conditionnement des chemins WAN. Le service d'optimisation WAN HCX est recommandé pour les déploiements qui ne sont pas en mesure de dédier des chemins 10 Gbit aux migrations. Dans les déploiements 10 Gbits à faible latence, l'utilisation de l'optimisation WAN peut ne pas améliorer les performances de migration. Pour plus d'informations, consultez Considérations relatives au déploiement du VMware HCX et meilleures pratiques.

Le service d'optimisation WAN HCX est déployé conjointement avec le dispositif de service d'interconnexion WAN HCX (HCX-IX). HCX-IX est responsable de la réplication des données entre l'environnement d'entreprise et l'environnement Amazon EVS.

Pour utiliser le service d'optimisation WAN HCX avec Amazon EVS, vous devez utiliser un groupe de ports distribués sur le sous-réseau VLAN HCX. Utilisez le groupe de ports distribués créé à l'étape précédente.

## (Facultatif) Activer le réseau optimisé pour la mobilité HCX

La mise en réseau optimisée pour la mobilité (MON) HCX est une fonctionnalité du service d'extension réseau HCX. Les extensions réseau non activées améliorent les flux de trafic pour les machines virtuelles migrées en permettant un routage sélectif au sein de votre environnement Amazon EVS. MON vous permet de configurer le chemin optimal pour migrer le trafic de charge de travail vers Amazon EVS lorsque vous étendez les réseaux de couche 2, en évitant ainsi un long chemin réseau aller-retour via la passerelle source. Cette fonctionnalité est disponible pour tous les déploiements Amazon EVS. Pour plus d'informations, consultez la section Configuration d'un réseau optimisé pour la mobilité dans le guide de l'utilisateur du VMware HCX.

> **Important**
>
> Avant d'activer HCX MON, lisez les limitations suivantes et les configurations non prises en charge pour HCX Network Extension.
> Restrictions et limitations relatives à l'extension du réseau
> Restrictions et limitations pour les topologies réseau optimisées pour la mobilité

> **Important**
>
> Avant d'activer HCX MON, assurez-vous que dans l'interface NSX, vous avez configuré la redistribution de routes pour le CIDR du réseau de destination. Pour plus d'informations, consultez la section Configurer le BGP et la redistribution de routes dans la documentation de VMware NSX.

## Vérifiez la connectivité HCX

VMware HCX inclut des outils de diagnostic intégrés qui peuvent être utilisés pour tester la connectivité. Pour plus d'informations, consultez la section Résolution des problèmes liés au VMware HCX dans le Guide de l'utilisateur du VMware HCX.

# Configuration de la connectivité Internet publique HCX

Vous pouvez configurer l'accès public à Internet pour votre VLAN public HCX en associant des adresses IP élastiques à votre VLAN. Cela permet une connectivité Internet directe pour les appliances VMware HCX et les charges de travail qui nécessitent un accès Internet pour les opérations de migration.

## Rubriques en relation

Cette rubrique couvre la gestion de l'accès Internet pour le VLAN public HCX. Pour une mise en œuvre complète :

1. Complétez les prérequis dans. Configuration d'Amazon Elastic VMware Service
2. Configurez la configuration initiale dansPrise en main.
3. Configurer l'accès à Internet (cette rubrique).

# À propos de l'accès Internet VLAN HCX

Vous pouvez configurer l'accès à Internet pour les appareils VMware HCX, ce qui vous permet d'effectuer la migration HCX de vos charges de travail vers Amazon EVS via Internet.

Cette approche :

- Permet les migrations de machines virtuelles sans nécessiter de connectivité privée dédiée.
- Fournit une solution flexible et rentable pour la migration.

> **Important**
>
> La migration HCX via Internet n'est généralement pas recommandée pour :
>
> - Applications sensibles à l'instabilité ou à la latence du réseau.
> - Opérations vMotion critiques.
> - Migrations à grande échelle avec des exigences de performance strictes.
>
> Pour ces scénarios, nous vous recommandons d'utiliser la connectivité privée HCX. Une connexion dédiée privée offre des performances plus fiables que les connexions Internet.

## Vue d'ensemble de la connectivité Internet

Passez en revue les considérations suivantes.

### Exigences de mise en réseau HCX et DNAT

HCX présente des contraintes réseau spécifiques qui affectent la façon dont vous configurez l'accès public à Internet.

HCX ne prend pas en charge la traduction d'adresses réseau de destination (DNAT). HCX nécessite plutôt que le réseau de liaison montante soit routable avec une adresse IP de passerelle par défaut.

Les sous-réseaux VLAN Amazon EVS incluent une adresse IP de passerelle par défaut, comme les autres sous-réseaux VPC. Toutefois, ces sous-réseaux sont toujours des sous-réseaux privés, même lorsque vous utilisez des blocs CIDR en dehors de la RFC1918 plage d'adresses.

### Activation de la connectivité Internet HCX

Pour activer la connectivité Internet sans DNAT, Amazon EVS utilise une approche de configuration CIDR spécifique :

- Exigence d'adresse CIDR routable sur Internet : Amazon EVS nécessite une adresse CIDR routable sur Internet qui correspond à l'adresse CIDR de votre sous-réseau VLAN HCX.
- Allocation IPAM : Amazon EVS utilise un CIDR public alloué par IPAM avec une longueur de masque réseau minimale de /28 comme CIDR routable sur Internet.
- Configuration du VPC : vous devez ajouter manuellement le CIDR public alloué par IPam à votre VPC en tant que CIDR VPC secondaire.
- Déploiement du sous-réseau VLAN : une fois l'IPAM et le VPC configurés, vous pouvez utiliser le CIDR public alloué par l'IPAM dans le sous-réseau VLAN HCX lors du déploiement d'Amazon EVS.
- Configuration IP élastique : Amazon EVS nécessite la configuration suivante :
  - Allouer Elastic IPs : vous allouez Elastic IPs à partir du CIDR alloué par l'IPAM. Vous devez allouer au moins deux adresses IP élastiques (EIPs) depuis le pool IPAM pour les appliances HCX Manager et HCX Interconnect (HCX-IX). Allouez une adresse IP élastique supplémentaire pour chaque appliance réseau HCX que vous devez déployer.
  - Associer au VLAN : vous associez chaque adresse IP élastique que vous souhaitez utiliser avec une appliance HCX au sous-réseau VLAN HCX. Utilisez la console Amazon EVS ou AWS CLI pour cette association.
  - Configurer l'adresse de passerelle : La première adresse utilisable du CIDR devient l'adresse de passerelle que vous configurez dans votre appliance HCX.
  - Routage du trafic : le trafic pour chaque adresse IP élastique associée est acheminé directement vers l'appliance HCX de destination avec la même adresse IP, sans DNAT.

Pour savoir comment configurer HCX avec une connectivité Internet pour le déploiement de l'environnement Amazon EVS, consultez Configuration d'Amazon Elastic VMware Service et. Prise en main

## Considérations relatives au fonctionnement

- Le bloc CIDR du VLAN public HCX doit avoir une longueur de masque réseau /28.
- EIPs peuvent être associés ou dissociés du VLAN public HCX après le déploiement à l'aide de la console Amazon EVS ou AWS CLI, mais ils doivent provenir du même pool IPAM.
- Chaque association EIP possède son propre identifiant d'association unique.

- Vous pouvez en avoir jusqu' EIPs à 13 dans un pool IPAM public associé au VLAN public /28 HCX. Vous ne pouvez pas associer les deux premiers EIPs ou le dernier EIP du bloc CIDR public alloué par IPAM au sous-réseau VLAN public HCX. Elles EIPs sont réservées en tant qu'adresses réseau, passerelle par défaut et adresses de diffusion. Amazon EVS génère une erreur de validation si vous tentez de les EIPs associer au VLAN.

### Considérations sur la sécurité

- Les listes de contrôle d'accès réseau (ACLs) s'appliquent toujours au trafic passant par le sous-réseau VLAN public HCX.
- Les règles des groupes de sécurité ne s'appliquent pas au trafic sur les sous-réseaux VLAN publics HCX. Utilisez le réseau ACLs pour contrôler le trafic.

> **Important**
>
> Si vous vous connectez via Internet, l'association d'une adresse IP élastique à un VLAN fournit un accès Internet direct à toutes les ressources de ce VLAN. Assurez-vous que les listes de contrôle d'accès réseau appropriées sont configurées pour restreindre l'accès en fonction de vos exigences de sécurité.

## Gestion des adresses IP Elastic pour VLANs

Vous pouvez associer et dissocier des adresses IP élastiques à un VLAN public HCX à l'aide de la console Amazon EVS ou. AWS CLI

> **Note**
>
> Amazon EVS prend uniquement en charge l'association et la dissociation d'une adresse IP élastique à un VLAN public HCX pour le moment.

### Associer une adresse IP élastique à un VLAN

#### Conditions préalables

Vérifiez que vous disposez des éléments suivants :

- L'adresse IP élastique est allouée à partir du pool IPAM public appartenant à Amazon.
- L'environnement Amazon EVS est déjà créé.

Example

Amazon EVS console

1. Accédez à la console Amazon EVS.
2. Dans le menu de navigation, choisissez Environments.
3. Sélectionnez l'environnement.
4. Dans l'onglet Réseaux et connectivité, sélectionnez le VLAN public HCX.

> **Note**
>
> Amazon EVS prend uniquement en charge l'association EIPs avec le VLAN HCX pour le moment.

5. Choisissez Associer EIP au VLAN.
6. Sélectionnez la ou les adresses IP élastiques à associer au VLAN public HCX.
7. Choisissez Associer EIPs. Vous pouvez en EIPs associer jusqu'à 13 au VLAN public HCX.

> **Note**
>
> Vous ne pouvez pas associer les deux premiers EIPs du bloc CIDR IPAM public au sous-réseau VLAN. Elles EIPs sont réservées en tant qu'adresses réseau et de passerelle par défaut.

8. Vérifiez les associations EIP pour confirmer qu'elles EIPs ont été associées au VLAN public HCX.

AWS CLI

1. Pour associer une adresse IP élastique à un VLAN, utilisez l'exemple de `associate-eip-to-vlan` commande.
   - `environment-id`- L'ID de votre environnement Amazon EVS.

- `vlan-name`- Ça doit l'êtrehcx. Amazon EVS prend uniquement en charge l'association EIP avec le VLAN HCX pour le moment.
- `allocation-id`- L'ID d'allocation de l'adresse IP élastique.

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

La commande renvoie des détails sur le VLAN, y compris la nouvelle association 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"
    }
}
```

Le `eipAssociations` tableau montre la nouvelle association, notamment :

- `associationId`- L'identifiant unique de cette association EIP, utilisé pour la dissociation.
- `allocationId`- L'ID d'allocation de l'adresse IP élastique associée.
- `ipAddress`- L'adresse IP attribuée au VLAN.

2. Répétez l'étape pour en associer d'autres EIPs. Vous pouvez en EIPs associer jusqu'à 13 au VLAN public HCX.

## Dissocier une adresse IP élastique d'un VLAN

### Conditions préalables

Vérifiez que vous disposez des éléments suivants :

- L'environnement Amazon EVS est déjà créé.
- L'EIP est associé à l'environnement Amazon EVS.

### Example

#### Amazon EVS console

1. Accédez à la console Amazon EVS.
2. Dans le menu de navigation, choisissez Environments.
3. Sélectionnez l'environnement.
4. Dans l'onglet Réseaux et connectivité, sélectionnez le VLAN public HCX.
5. Choisissez Dissocier l'EIP du VLAN.
6. Sélectionnez la ou les adresses IP élastiques à dissocier du VLAN public HCX.

> **Important**
>
> La dissociation EIPs peut entraîner une perte de connectivité Internet pour les appareils qui utilisent des sous-réseaux VLAN publics.

7. Choisissez Dissocier EIPs.
8. Vérifiez les associations EIP pour confirmer qu'elles EIPs ont été dissociées du VLAN public HCX.

#### AWS CLI

Pour dissocier une adresse IP élastique d'un VLAN, utilisez l'exemple `disassociate-eip-from-vlan` de commande.

- `environment-id`- L'ID de votre environnement Amazon EVS.
- `vlan-name`- Ça doit l'êtrehcx. Amazon EVS prend uniquement en charge l'association EIP avec le VLAN HCX pour le moment.
- `association-id`- L'ID d'association de l'association EIP à supprimer.

> **Important**
>
> La dissociation EIPs peut entraîner une perte de connectivité Internet pour les appareils qui utilisent des sous-réseaux VLAN publics.

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

La commande renvoie des informations sur le VLAN dont l'association EIP a été supprimée :

```
{
    "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"
    }
}
```

Le `eipAssociations` tableau vide confirme que l'adresse IP élastique a été correctement dissociée du VLAN.

# À propos de l'optimisation du WAN HCX pour les migrations basées sur Internet

> **Note**
>
> La fonctionnalité d'optimisation WAN n'est plus disponible dans HCX 4.11.3. Pour plus d'informations, consultez les notes de mise à jour de HCX 4.11.3.

Lorsque vous effectuez des migrations via Internet, l'optimisation du WAN HCX (HCX-WO) peut améliorer les performances de migration. Le service fonctionne conjointement avec l'appliance HCX Interconnect (HCX-IX) pour :

- Appliquez des techniques de réduction des données pour minimiser l'utilisation de la bande passante.
- Mettez en œuvre le conditionnement des chemins WAN pour optimiser les performances du réseau.
- Améliorez les vitesses de migration sur les connexions Internet à latence élevée.
- Améliorez la fiabilité des migrations basées sur Internet.

L'optimisation du WAN HCX est particulièrement utile pour les migrations basées sur Internet lorsque :

- La latence du réseau peut être supérieure à celle des options de connectivité privée.
- La bande passante disponible peut être limitée ou variable.
- Les conditions du réseau peuvent fluctuer en raison des modèles de trafic Internet.

Pour obtenir des instructions détaillées sur la configuration de l'optimisation du réseau WAN HCX après avoir configuré la connectivité Internet, consultezthe section called “(Facultatif) Configurer l'optimisation du réseau WAN HCX”.

> **Note**
>
> Bien que l'optimisation du WAN puisse améliorer de manière significative les performances de migration via Internet, elle peut ne pas apporter d'avantages supplémentaires dans les

environnements dotés de connexions 10 Gbits dédiées à faible latence. Tenez compte des caractéristiques de votre réseau lorsque vous décidez d'activer ou non cette fonctionnalité.

# Gestion des environnements Amazon EVS

Ce chapitre inclut les rubriques suivantes pour vous aider à gérer votre environnement.

- the section called "Abonnements VCF"- Décrit le fonctionnement des abonnements VCF avec Amazon EVS et les responsabilités des clients en matière de gestion des abonnements VCF.
- the section called "Versions et EC2 instances VCF"- Décrit les versions VCF et ESX prises en charge et explique comment vérifier la disponibilité des versions dans Amazon EVS.
- the section called "Gestion du cycle de vie"- Décrit les responsabilités en matière de gestion du cycle de vie au sein d'un environnement Amazon EVS, y compris la gestion de l'infrastructure sous-jacente, la gestion des mises à niveau VCF et la gestion du cycle de vie des hôtes ESX.
- the section called "Maintien de l'environnement"- Décrit comment effectuer les tâches de maintenance courantes pour votre environnement Amazon EVS, notamment la configuration réseau, la maintenance de l'hôte ESX, la vérification de l'état de l'environnement et la gestion de calendriers de rotation secrets pour vos informations d'identification VCF.
- the section called "Créer un hôte"- Décrit comment créer un hôte Amazon EVS après le déploiement de l'environnement et comment ajouter l'hôte au cluster.
- the section called "Supprimer l'hôte"- Décrit comment supprimer un hôte Amazon EVS et le retirer du cluster.

## Abonnements VCF

> **Note**
>
> Amazon EVS ne prend pas en charge les licences vSphere perpétuelles. Vous devez disposer d'un abonnement VMware Cloud Foundation valide et actif pour utiliser Amazon EVS.

Amazon EVS utilise des abonnements VMware Cloud Foundation (VCF) avec des droits de portabilité des licences que vous apportez à AWS (BYOS). Pour déployer correctement un environnement Amazon EVS, vous devez fournir une clé de solution VCF valide et une clé de licence vSAN dans la demande de création de l'environnement. La clé de licence vSphere sert de clé de solution pour VCF. Chaque clé de licence VCF ne peut être utilisée que pour un seul environnement

Amazon EVS. La création de l'environnement échoue si vous essayez d'utiliser une clé de licence VCF déjà utilisée dans un autre environnement.

Votre clé de solution VCF doit comporter au moins 256 cœurs afin de fournir une capacité de base adéquate pour les quatre EC2 hôtes i4i.metal initiaux qu'Amazon EVS déploie lors de la création de l'environnement. Chaque hôte i4i.metal nécessite 64 cœurs. La clé de licence vSAN doit avoir au moins 110 TiB de capacité vSAN. La création de l'environnement échoue si vous essayez d'utiliser des clés de licence trop petites.

> **Note**
>
> Votre abonnement VCF sera disponible sur Amazon EVS dans toutes les AWS régions pour garantir la conformité des licences. Amazon EVS ne valide pas les clés de licence. Pour valider les clés de licence, consultez le support de Broadcom.

> **Note**
>
> Les informations relatives à votre logiciel VCF dans Amazon EVS seront partagées avec Broadcom afin de vérifier la conformité des licences.

## Gestion des abonnements

Vous êtes responsable de la gestion de vos abonnements VCF. Vos abonnements VCF doivent être gérés dans SDDC Manager. La suppression de vos clés de licence de SDDC Manager ou leur remplacement par une clé de licence en cours d'utilisation entraînera un échec de la vérification de l'état de l'environnement, vous empêchant ainsi d'ajouter des hôtes à votre environnement Amazon EVS. Pour plus d'informations sur les contrôles de l'état de l'environnement, the section called “Surveiller l'état de l'environnement” etthe section called “Résoudre les problèmes liés aux échecs des vérifications de l'état de”. Pour plus d'informations sur les clés de licence VCF, consultez la section Gestion des clés de licence dans VMware Cloud Foundation dans la documentation de VMware Cloud Foundation.

> **Important**
>
> Utilisez l'interface utilisateur du SDDC Manager pour gérer la solution VCF et les clés de licence vSAN. Amazon EVS exige que vous conserviez des clés de solution VCF et de

licence vSAN valides dans SDDC Manager pour que le service fonctionne correctement. Bien que les clés doivent être attribuées à vos hôtes et à votre cluster vSAN à l'aide de vSphere Client, vous devez vous assurer que ces clés apparaissent également dans l'écran de licence de l'interface utilisateur de SDDC Manager.

## Ajouter des clés de licence VCF

Sur le portail d'assistance de Broadcom, vous pouvez acheter des clés de licence VCF supplémentaires, diviser les clés de licence si vous possédez déjà de grandes clés ou fusionner plusieurs clés de licence. Cela vous permet d'octroyer des licences aux hôtes que vous avez ajoutés à votre environnement après le déploiement initial ou d'octroyer des licences à des environnements supplémentaires. Assurez-vous que les clés de licence achetées sont ajoutées dans l'inventaire de vCenter Server et de SDDC Manager. Si vous ajoutez des hôtes, assurez-vous que vos licences sont attribuées aux hôtes appropriés dans vSphere et qu'elles disposent de cœurs et d'une capacité de stockage vSAN adéquats. Amazon EVS ne prend pas en charge les hôtes sans licence. Pour plus d'informations, consultez la section Configuration des paramètres de licence pour les actifs dans vSphere Client dans la VMware documentation.

Les nouvelles clés de licence non expirées doivent être attribuées à vCenter Server avant l'expiration de la période d'évaluation de la clé de licence pour rester actives. Des clés de licence actives sont nécessaires pour configurer correctement un environnement Amazon EVS. Votre environnement ne pourra pas se déployer si une clé de licence expirée est fournie. Pour plus d'informations sur la création de clés de licence VCF, consultez la section Créer une nouvelle licence dans la VMware documentation. Si vous rencontrez des problèmes avec les clés de licence que vous avez ajoutées, consultezthe section called “La vérification de la couverture des clés a échoué”.

## Supprimer les clés de licence VCF

Vous pouvez supprimer les clés de licence VCF de l'inventaire du gestionnaire SDDC afin de réduire la capacité de votre cœur et de votre vSAN après avoir supprimé des hôtes de votre environnement. Pour rester en conformité avec les modèles de licence des produits que vous utilisez avec vSphere, vous devez supprimer toutes les clés de licence non attribuées de l'inventaire. Si vous avez divisé, fusionné ou mis à niveau des clés de licence dans le portail de support de Broadcom, vous devez supprimer les anciennes clés de licence. Pour plus d'informations, voir Supprimer une licence dans la VMware documentation.

# Versions VCF et types d' EC2 instances fournis par Amazon EVS

Amazon EVS fournit plusieurs versions de VMware Cloud Foundation (VCF), ESX et des types d' EC2 instances que vous pouvez sélectionner lors de la création d'un environnement et de la création d'un hôte.

## Vérification des versions VCF, des versions ESX et EC2 des types d'instances fournis

La AWS console affiche la liste des versions VCF fournies par Amazon EVS dans l'assistant de création d'environnement. Les versions ESX disponibles sont visibles lorsque vous sélectionnez un type d'instance lors de l'ajout d'un hôte à un environnement existant. Vous pouvez également afficher les versions VCF, les versions ESX et les types d' EC2 instances à l'aide de la CLI.

Example

Amazon EVS console

1. Accédez à la console Amazon EVS.
2. Dans le menu de navigation, choisissez Environments.
3. Effectuez l'une des actions suivantes :

   Pour vérifier les versions de VCF :

   a. Sélectionnez Créer un environnement.
   b. Dans le cadre des exigences de validation d'Amazon EVS, choisissez votre version VCF pour voir si le statut est disponible ou restreint pour vous.

   Pour vérifier les versions d'ESX :

   a. Sélectionnez un environnement existant.
   b. Choisissez Create host (Créer un hôte).
   c. Sélectionnez un type d'instance pour voir les versions ESX disponibles.

AWS CLI

Exécutez la commande suivante pour récupérer des informations sur les versions VCF et ESX :

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

Exemple de réponse :


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


> **Note**
>
> Si la version dont vous avez besoin s'affiche `RESTRICTED` et que vous avez un besoin particulier, consultez the section called "Demande d'accès aux versions limitées de VCF" pour plus d'informations sur la façon d'accéder à cette version.

## Versions VCF actuelles dans Amazon EVS

Amazon EVS fournit actuellement les versions VCF suivantes pour la création d'environnements :

| Version VCF | Version ESX par défaut | Statut | EC2 types d'instances |
|---|---|---|---|
| VCF-5.2.2 | ESXi-8,0U3G-24859861 | DISPONIBLE | i4i.metal |
| VCF-5.2.1 | ESXi-8,0U3B-24280767 | LIMITÉ | i4i.metal |

> **Note**
>
> Lorsque vous créez un nouvel environnement Amazon EVS, vous devez spécifier une version VCF.

## Considérations relatives à la version d'ESX

Chaque version VCF possède une version ESX par défaut basée sur la nomenclature Broadcom VCF (BOM). Lorsque vous créez un nouvel environnement, vous ne pouvez pas choisir une version spécifique d'ESX. La version ESX par défaut pour la version VCF sélectionnée est appliquée automatiquement.

Toutefois, lorsque vous ajoutez un hôte à votre environnement, vous pouvez sélectionner une version d'ESX disponible pour le type d'instance que vous avez choisi. Si vous n'en spécifiez aucune, Amazon EVS utilise la version ESX par défaut associée à la version VCF de votre environnement.

Une fois qu'un hôte a été ajouté, sa version ESX ne peut être mise à niveau qu'à l'aide de vCenter Lifecycle Manager.

> **Note**
>
> Amazon EVS ne fournit pas toutes les versions de VCF et ESX publiées par Broadcom. Pour obtenir des informations sur l'interopérabilité logicielle, reportez-vous à la matrice d'interopérabilité Broadcom. Pour une compatibilité matérielle complète avec AWS EC2 les instances, reportez-vous au Guide de compatibilité Broadcom.

## Demande d'accès aux versions limitées de VCF

Si vous avez besoin d'accéder à une version VCF dotée d'un `RESTRICTED` statut, contactez le AWS Support en fournissant les informations suivantes :

- L'identifiant AWS de votre compte
- La AWS région
- La version VCF spécifique dont vous avez besoin
- Votre cas d'utilisation et votre justification commerciale (par exemplesecurity/compliance, compatibility/dependency, et autres)

AWS Support examinera votre demande et approuvera ou demandera des informations supplémentaires. Après approbation, le statut de la version passera à celui indiqué `AVAILABLE` dans la réponse de la AWS console ou de `get-versions` l'API.

# Gestion du cycle de vie de l'environnement Amazon EVS

Cette page décrit vos responsabilités en matière de gestion du cycle de vie au sein d'un environnement Amazon EVS.

L'un des principaux avantages d'Amazon EVS est que vous avez le contrôle total de votre VMware architecture dans le cloud. Vous pouvez optimiser la VMware suite logicielle Cloud Foundation (VCF) pour répondre aux exigences uniques de vos applications. Amazon EVS étant un service autogéré, vous êtes responsable de la gestion du cycle de vie et de la maintenance des VMware logiciels utilisés dans l'environnement Amazon EVS, tels que ESX, vSphere, vSAN, NSX et SDDC Manager. Vous êtes également responsable de la maintenance de toutes les intégrations tierces, telles que les solutions de protection des données que vous intégrez à vos hôtes Amazon EVS.

Vous êtes responsable de la configuration des composants AWS réseau sous-jacents utilisés par Amazon EVS, notamment les tables de routage VPC, les règles des groupes de sécurité et des listes de contrôle d'accès réseau (ACL), la configuration du serveur de routage VPC, les passerelles Internet, les passerelles NAT et les passerelles de transit (pour la connectivité sur site).

AWS est responsable du déploiement de l'environnement Amazon EVS avec les configurations réseau que vous fournissez. Le déploiement de l'environnement inclut les éléments suivants :

- Démarrage de la configuration réseau de votre environnement Amazon EVS.
- Activation du routage nord-sud avec l'instance de serveur de routage VPC que vous fournissez.

- Déploiement des sous-réseaux VLAN EVS requis, des interfaces réseau élastiques et des quatre hôtes ESX initiaux.
- Configuration d'un réseau superposé NSX avec une passerelle de niveau 0 et une passerelle de niveau 1.
- Déploiement d'un cluster NSX Edge avec deux nœuds NSX Edge en Active/Standby mode.
- Création et configuration du cluster vSAN initial et montage de la banque de données.

Vous êtes responsable de la configuration de VMware NSX, notamment des segments réseau, des règles de pare-feu distribuées et des équilibreurs de charge. Vous êtes également responsable de la configuration de toutes les solutions intégrées que vous implémentez avec Amazon EVS après le déploiement de l'environnement EVS, y compris la configuration VMware HCX et les passerelles NSX Tier-1 supplémentaires.

Pour plus d'informations sur les responsabilités AWS des clients et pour en savoir plus, consultez le modèle de responsabilitéAWS partagée.

> **Note**
>
> Une passerelle de niveau 0 et une passerelle de niveau 1 sont créées et configurées dans le cadre du déploiement de l'environnement Amazon EVS. Amazon EVS ne prend en charge qu'une seule passerelle de niveau 0 pour le moment. Toute modification apportée à ces routeurs logiques ou au nœud NSX Edge VMs peut affecter la connectivité et doit être évitée.

## VMware mises à jour logicielles

> **Warning**
>
> Si vous avez mis à jour votre version d'ESX après le déploiement de l'environnement Amazon EVS, le gestionnaire SDDC peut échouer lors de la validation de l'hôte VCF à l'étape des hôtes de commission. Pour connaître les étapes à suivre pour résoudre ce problème, consultezthe section called “Le gestionnaire SDDC échoue à la validation de l'hôte VCF lors de la mise en service de l'hôte”.

Pour plus d'informations sur les versions VCF fournies par Amazon EVS, consultez. the section called “Versions et EC2 instances VCF” Conformément au modèle de responsabilitéAWS partagée,

vous êtes responsable de l'application des correctifs, mises à jour ou mises à niveau du logiciel VCF, y compris ESX, vCenter Server, vSAN, NSX, SDDC Manager et d'autres solutions intégrées, dans votre environnement EVS. Après le déploiement, nous vous recommandons de consulter la version du logiciel VCF déployée par Amazon EVS et de la mettre à jour si nécessaire. Vous pouvez obtenir les mises à jour du VCF via le portail d'assistance de Broadcom. Nous vous recommandons également d'établir et de respecter un calendrier de maintenance régulier pour les mises à jour et les correctifs.

> **Note**
>
> Amazon EVS ne prend pas en charge VMware Cloud Foundation 9 pour le moment.

> **Note**
>
> Amazon EVS ne fournit pas toutes les versions de VCF et ESX publiées par Broadcom. Pour obtenir des informations sur l'interopérabilité logicielle, reportez-vous à la matrice d'interopérabilité Broadcom. Pour une compatibilité matérielle complète avec AWS EC2 les instances, reportez-vous au Guide de compatibilité Broadcom.

Certains correctifs, mises à jour ou mises à niveau peuvent avoir un impact sur les charges de travail exécutées dans votre environnement. Avant d'appliquer des correctifs, de mettre à jour ou de mettre à niveau votre logiciel VCF, nous vous recommandons de consulter le guide de gestion du cycle de vie VCF pour comprendre l'impact de ces modifications sur votre environnement. Nous vous recommandons également de tester les modifications dans un environnement intermédiaire avant de les déployer en production. Vous pouvez consulter les notes de mise à jour de VCF 5.2.x pour comprendre les dernières mises à jour de VCF 5.2.x.

## Cycle de vie et maintenance de l'hôte ESX

Vous êtes responsable de la gestion et de la maintenance du cycle de vie des hôtes ESX au sein de l'environnement Amazon EVS, notamment de la surveillance de l'état de santé de l'hôte et de la résolution des problèmes liés à l'hôte. Pour de plus amples informations, veuillez consulter the section called “Maintien de l'environnement”.

AWS effectue une maintenance planifiée sur les EC2 instances i4i.metal sous-jacentes afin de garantir la fiabilité, la disponibilité et les performances de l'infrastructure. Pour de plus amples

informations, veuillez consulter the section called "À propos de la maintenance AWS planifiée pour les EC2 instances".

# Réalisation de la maintenance de votre environnement

Cette section décrit comment effectuer des tâches de maintenance courantes pour votre environnement Amazon EVS.

Rubriques

- Surveillez l'état et les ressources de votre environnement
- Maintenance de l'AMI
- Maintenance de l'hôte Amazon EVS
- Configuration d'une table de routage personnalisée pour les sous-réseaux Amazon EVS
- Configuration d'une liste de contrôle d'accès réseau pour contrôler le trafic du sous-réseau Amazon EVS VLAN
- Cycle de vie de gestion des secrets

## Surveillez l'état et les ressources de votre environnement

Vous pouvez surveiller différents aspects de votre environnement Amazon EVS et des AWS ressources sous-jacentes à l'aide de la console Amazon EVS ou. AWS CLI

> **Note**
>
> VMware Les composants Cloud Foundation (VCF) sont surveillés dans SDDC Manager. Vous ne pouvez pas surveiller les composants VCF à l'aide de la console Amazon EVS ou. AWS CLI Pour plus d'informations sur l'utilisation de SDDC Manager pour surveiller les composants de VMware Cloud Foundation (VCF), consultez Getting started with SDDC Manager.

### Afficher l'état de l'environnement et les ressources

L'état de l'environnement vous aide à déterminer si votre environnement présente des problèmes nécessitant une attention particulière. Suivez cette procédure pour vérifier l'état de votre environnement et consulter les ressources sous-jacentes.

Example

Amazon EVS console

1. Ouvrez la console Amazon EVS.
2. Dans le panneau de navigation, choisissez Environments (Environnements).
3. Choisissez votre ID d'environnement pour ouvrir la page des détails de l'environnement.
4. Sous Détails, consultez l'état de l'environnement.

   Si votre environnement est en bon état, le statut indique « Réussi ». En cas de problème, le statut est indiqué comme Échec. Lorsque le statut est Échoué, vous pouvez afficher une fenêtre contextuelle qui affiche les résultats de quatre vérifications de l'état de l'environnement :

   - Réutilisation de la clé : affiche « Passée » ou « Échec » pour indiquer si la clé de licence VCF est valide.
   - Nombre d'hôtes : affiche Inconnu, Réussi ou Échec pour indiquer l'état de la connectivité de l'hôte.
   - Couverture de la clé : affiche « Passée » ou « Échec » pour indiquer si la clé de licence VCF couvre tous les hôtes.
   - Accessibilité : affiche « réussi » ou « échec » pour indiquer que SDDC Manager est joignable.

     Pour plus d'informations sur le dépannage des échecs de vérification de l'état de l'environnement, consultezRésolution des problèmes.

     Pour consulter les ressources de votre environnement

     Choisissez l'un des onglets suivants :

   - Hôtes : affiche les hôtes de votre environnement.
   - Réseaux et connectivité : affiche les ressources du VPC, des sous-réseaux EVS et du serveur de routage VPC associées à votre environnement.
   - Appliances de gestion : affiche les appliances de gestion VCF de votre environnement avec leurs noms d'hôte DNS et les informations d'identification associées.
   - Balises : affiche les balises associées à votre environnement.

AWS CLI

Vous pouvez utiliser le AWS CLI pour vérifier l'état de votre environnement et de vos ressources.

Pour répertorier tous les environnements et leur état

```
aws evs list-environments
```

> **Tip**
>
> Utilisez le `--query` paramètre pour filtrer la sortie. Par exemple :

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

Pour répertorier les hôtes de l'environnement

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

Pour répertorier l'environnement VLANs

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

Pour plus d'informations sur les opérations d'API, consultez les informations suivantes dans le guide de référence des API Amazon EVS :

- ListEnvironments
- ListEnvironmentHosts
- ListEnvironmentVlans

## Maintenance de l'AMI

Amazon EVS déploie des hôtes ESX avec une Amazon Machine Image (AMI) EVS personnalisée. L'AMI contient un module complémentaire de fournisseur personnalisé contenant les packages requis pour exécuter ESX sur Amazon EC2.

### Résoudre les problèmes liés à l'ajout d'un hôte en raison d'une image de cluster incompatible

Lorsque vous ajoutez un hôte à votre environnement, celui-ci dispose de la dernière version disponible du module complémentaire EVS Custom Vendor. Si votre environnement utilise des hôtes dotés d'une ancienne version du module complémentaire, l'ajout de nouveaux hôtes échoue avec un message d'erreur indiquant que le nouvel hôte n'est pas compatible avec votre image de cluster. Pour connaître les étapes détaillées permettant de résoudre ce problème, consultezthe section called "Ajouter une défaillance de l'hôte due à une image de cluster incompatible".

## Maintenance de l'hôte Amazon EVS

Amazon EVS étant un service autogéré, vous êtes responsable de la maintenance du logiciel VMware Cloud Foundation (VCF) qui s'exécute sur l'hôte, de la surveillance de l'état de l'hôte et de la résolution des problèmes liés à l'hôte, y compris le remplacement de l'hôte en cas de défaillance de l'hôte. Pour plus d'informations sur la gestion des hôtes ESX dans VMware Cloud Foundation (VCF), consultez la section Gestion des hôtes dans la documentation de VMware Cloud Foundation.

### Vérification de l'état de santé de l' EC2 instance sous-jacente

Amazon EC2 effectue des contrôles automatisés sur chaque EC2 instance en cours d'exécution afin d'identifier les problèmes matériels et logiciels. Vous pouvez consulter les résultats de ces vérifications d'état dans la EC2 console ou AWS CLI pour identifier des problèmes spécifiques et détectables. Pour plus d'informations, consultez Afficher les vérifications de statut pour une EC2 instance Amazon dans le guide de l' EC2 utilisateur Amazon et describe-instance-statusdans le manuel de référence de ligne de AWS CLI commande.

Vous pouvez créer une CloudWatch alarme pour vous avertir si les vérifications d'état échouent sur une instance spécifique. Pour plus d'informations, consultez la section Créer des CloudWatch alarmes pour les EC2 instances Amazon qui échouent aux vérifications de statut dans le guide de EC2 l'utilisateur Amazon.

### À propos de la maintenance AWS planifiée pour les EC2 instances

AWS effectue une maintenance planifiée sur les EC2 instances sous-jacentes afin de garantir la fiabilité, la disponibilité et les performances. EC2 les instances bare metal sont soumises aux mêmes types d'événements planifiés que les autres EC2 instances. AWS peut planifier des événements pour redémarrer, arrêter et mettre hors service vos instances en raison de problèmes matériels

sous-jacents ou d'une maintenance planifiée. Ces événements ne se produisent pas fréquemment. Pour plus d'informations, consultez la section Types d'événements planifiés dans le guide de EC2 l'utilisateur Amazon.

> **Note**
>
> Vous devez placer vos hôtes en mode maintenance dans vSphere Client avant tout événement de redémarrage planifié.

Si l'une de vos instances est affectée par un événement programmé, vous en AWS informera à l'avance par e-mail, en utilisant l'adresse e-mail associée à votre Compte AWS. AWS envoie également un événement AWS Health, que vous pouvez surveiller et gérer à l'aide d'Amazon EventBridge. Pour plus d'informations, consultez les sections Surveillance des événements dans AWS Health with Amazon EventBridge et Événements planifiés pour les EC2 instances Amazon dans le guide de EC2 l'utilisateur Amazon.

À tout moment, vous pouvez reprogrammer l'événement afin qu'il ait lieu à la date et à l'heure qui vous conviennent. L'événement peut être reprogrammé jusqu'à la date d'échéance de celui-ci. Pour plus d'informations, consultez la section Replanifier un événement planifié pour une EC2 instance dans le guide de  EC2 l'utilisateur Amazon.

### Utilisation des réservations de capacité EC2 à la demande

Vous pouvez utiliser les réservations de capacité à EC2 la demande pour vous assurer que votre cluster dispose d'une capacité suffisante pendant les périodes de maintenance. Vous pouvez réserver des capacités dans une zone de disponibilité spécifique pour n'importe quelle durée. Pour plus d'informations, consultez la section Réserver une capacité de calcul avec des réservations de capacité EC2 à la demande dans le guide de EC2 l'utilisateur Amazon.

Pour savoir comment créer une réservation de capacité, consultez la section Créer une réservation de capacité dans le guide de EC2 l'utilisateur Amazon.

> **Note**
>
> Si vous utilisez des réservations de capacité EC2 à la demande ou des hôtes EC2 dédiés, nous vous recommandons de conserver un hôte de rechange pour les charges de travail critiques. Alors que les réservations de capacité vous garantissent l'accès à une quantité

spécifique de capacité d' EC2 instance dans une zone de disponibilité donnée, le fait de disposer d'un hôte de rechange fournit une couche supplémentaire de redondance essentielle pour les charges de travail critiques. Pour les hôtes dédiés, le fait de disposer d'un hôte de rechange garantit le maintien de l'environnement pour les charges de travail critiques, même si un hôte principal nécessite une maintenance ou rencontre un problème.

## Préparation du AWS calendrier **`system-maintenance`** et des **`instance-retirement`** événements

AWS planifie deux types d'`system-maintenance`événements : la maintenance du réseau et la maintenance de l'alimentation.

- Lors d'une maintenance du réseau, les instances planifiées perdent leur connectivité réseau pendant une courte période. La connectivité réseau normale vers votre instance est restaurée une fois la maintenance terminée.
- Lors d'une maintenance de l'alimentation, les instances planifiées sont mises hors ligne pendant une courte période, puis redémarrées. Lorsqu'un redémarrage est effectué sur des instances EC2 bare metal, les données du volume de stockage d'instance ne sont pas conservées.

AWS planifie les EC2 `instance-retirement` événements lorsqu'une dégradation du matériel sous-jacent hébergeant vos EC2 instances est détectée.

Pour remédier `system-maintenance` aux `instance-retirement` événements, remplacez l'hôte défaillant par un nouvel hôte à l'aide de la console Amazon EVS ou AWS CLI du SDDC Manager avant que l'événement de maintenance ne se produise. Si vous attendez que l'événement de maintenance se produise et qu'un redémarrage de l' EC2 instance soit nécessaire, vous perdrez les données vSAN stockées sur le volume de stockage de l'instance. Pour obtenir des instructions complètes, consultez the section called “Remplacer un hôte Amazon EVS”.

**Important**

La EC2 console ne doit pas être utilisée pour gérer l'état de vos hôtes Amazon EVS, notamment pour les arrêter, les démarrer et les arrêter. N'essayez pas de démarrer, d'arrêter ou de mettre hors service les EC2 instances déployées par Amazon EVS. Cette action entraîne une perte de données vSAN.

## Remplacer un hôte Amazon EVS

Suivez cette procédure pour remplacer un hôte Amazon EVS.

> **Warning**
>
> Les hôtes Amazon EVS utilisent un module complémentaire de fournisseur personnalisé pour fournir des fonctionnalités d'hôte importantes. Lorsque vous ajoutez un hôte à votre environnement, il dispose de la dernière version disponible du module complémentaire personnalisé Amazon EVS. Si votre environnement utilise des hôtes dotés d'une ancienne version du module complémentaire, l'ajout d'un hôte à votre cluster vSphere entraînera l'échec de la correction de l'image du cluster. Pour connaître les étapes à suivre pour résoudre ce problème, consultezthe section called “Résoudre les problèmes liés à l'ajout d'un hôte en raison d'une image de cluster incompatible”.

> **Warning**
>
> Si vous avez mis à jour votre version d'ESX après le déploiement, le gestionnaire SDDC peut échouer lors de la validation de l'hôte VCF à l'étape des hôtes de commission. Pour connaître les étapes à suivre pour résoudre ce problème, consultezthe section called “Le gestionnaire SDDC échoue à la validation de l'hôte VCF lors de la mise en service de l'hôte”.

> **Note**
>
> Assurez-vous que le nombre d'hôtes Amazon EVS par quota d'environnement EVS est correctement défini pour garantir la réussite de la création d'hôtes. La création d'hôtes échoue si cette valeur de quota est inférieure au nombre d'hôtes que vous essayez de configurer au sein d'un même environnement Amazon EVS. Il se peut que vous deviez demander une augmentation du quota pour les opérations de maintenance nécessitant le remplacement de l'hôte. Pour de plus amples informations, veuillez consulter Quotas de service.

Example

Amazon EVS console and SDDC Managuer UI

1. Accédez à la console Amazon EVS.
2. Dans le volet de navigation, choisissez Environment.
3. Sélectionnez l'environnement qui contient l'hôte à remplacer.
4. Sélectionnez l'onglet Hosts.
5. Choisissez Create host (Créer un hôte).
6. Spécifiez les détails de l'hôte et choisissez Create host.
7. Pour vérifier que l'opération est terminée, vérifiez que l'état de l'hôte est passé à Créé.
8. Récupérez les informations d'identification du mot de passe root ESX dans AWS Secrets Manager. Pour plus d'informations sur la récupération de secrets, consultez la section Obtenir des AWS secrets depuis Secrets Manager dans le guide de l'utilisateur de AWS Secrets Manager.
9. Accédez à SDDC Manager.
10. Mettez en service le nouvel hôte dans SDDC Manager, en utilisant les informations d'identification racine ESX que vous avez récupérées lors d'une étape précédente. Pour plus d'informations, consultez Commission Hosts dans la documentation de VMware Cloud Foundation.
11. Ajoutez le nouvel hôte au cluster. Pour plus d'informations, consultez Comment ajouter un hôte ESX à votre cluster vSphere à l'aide du flux de travail Quickstart dans la documentation de vSphere.
12. Mettez hors service l'ancien hôte de SDDC Manager que vous souhaitez supprimer de SDDC Manager. Pour plus d'informations, consultez la section Démission des hôtes dans la documentation de VMware Cloud Foundation.
13. Retournez à la console Amazon EVS.
14. Dans l'onglet Hôtes, sélectionnez l'hôte défaillant et choisissez Supprimer > Supprimer l'hôte.

AWS CLI and SDDC Manager UI

1. Ouvrez une nouvelle session de terminal.
2. Créez un nouvel hôte. Voir l'exemple de commande ci-dessous pour référence.

```
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. Récupérez les informations d'identification du mot de passe root ESX dans AWS Secrets Manager. Pour plus d'informations sur la récupération de secrets, consultez la section Obtenir des AWS secrets depuis Secrets Manager dans le guide de l'utilisateur de AWS Secrets Manager.
4. Accédez à SDDC Manager.
5. Mettez en service le nouvel hôte dans SDDC Manager, en utilisant les informations d'identification racine ESX que vous avez récupérées lors d'une étape précédente. Pour plus d'informations, consultez Commission Hosts dans la documentation de VMware Cloud Foundation.
6. Ajoutez le nouvel hôte au cluster qui contient l'hôte défaillant.
7. Mettez hors service l'hôte défaillant dans le gestionnaire SDDC. Pour plus d'informations, consultez la section Démission des hôtes dans la documentation de VMware Cloud Foundation.
8. Retournez au terminal.
9. Supprimez l'hôte défaillant. Voir l'exemple de commande ci-dessous pour référence.

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

## Résolution des problèmes

Pour obtenir des conseils de dépannage, consultezRésolution des problèmes. Si vous continuez à rencontrer des problèmes après avoir lu les instructions de dépannage, contactez le AWS Support pour obtenir de l'aide.

## Configuration d'une table de routage personnalisée pour les sous-réseaux Amazon EVS

Amazon EVS prend en charge l'utilisation d'une table de routage personnalisée uniquement après la création de l'environnement Amazon EVS. Pour que la création d'un environnement soit réussie, vous devez configurer la table de routage principale pour autoriser le trafic vers les services dépendants tels que le DNS et les systèmes sur site. Cela est dû au fait que les sous-réseaux VLAN Amazon EVS sont implicitement associés à la table de routage principale de notre VPC lors du déploiement de l'environnement.

Une fois votre environnement déployé, vous devez associer explicitement chacun des sous-réseaux Amazon EVS VLAN à une table de routage dans votre VPC. La connectivité NSX échoue si vos sous-réseaux VLAN ne sont pas explicitement associés à une table de routage VPC. Nous vous recommandons vivement d'associer explicitement vos sous-réseaux à une table de routage personnalisée. Une table de routage personnalisée fournit un contrôle plus précis du routage du trafic réseau au sein de votre VPC, ce qui permet de définir des règles de routage personnalisées pour des sous-réseaux ou des passerelles spécifiques. Pour plus d'informations sur la création d'une table de routage personnalisée, consultez la section Créer une table de routage pour votre VPC dans le guide de l'utilisateur Amazon VPC.

## Configuration d'une liste de contrôle d'accès réseau pour contrôler le trafic du sous-réseau Amazon EVS VLAN

Une liste de contrôle d'accès (ACL) réseau autorise ou refuse un trafic entrant ou sortant spécifique au niveau du sous-réseau. Vous pouvez utiliser le réseau ACLs pour contrôler le trafic entrant et sortant pour vos sous-réseaux Amazon EVS VLAN. Pour plus d'informations, consultez la section Créer une ACL réseau pour votre VPC dans le guide de l'utilisateur Amazon VPC.

> **Important**
>
> EC2 les groupes de sécurité ne fonctionnent pas sur les interfaces réseau élastiques connectées aux sous-réseaux Amazon EVS VLAN. Pour contrôler le trafic à destination et en provenance des sous-réseaux VLAN Amazon EVS, vous devez utiliser une liste de contrôle d'accès réseau.

**Warning**

Amazon EVS nécessite l'accès à votre déploiement VCF. Vous devez configurer vos groupes de sécurité et vos listes de contrôle d'accès réseau (ACLs) pour permettre à Amazon EVS de communiquer avec :

- Serveurs DNS via TCP/UDP le port 53.
- Sous-réseau VLAN de gestion de l'hôte via HTTPS et SSH.
- Sous-réseau VLAN de la machine virtuelle de gestion via HTTPS et SSH.

Si vos groupes de sécurité et votre réseau n' ACLs autorisent pas cet accès, le déploiement de l'environnement Amazon EVS échouera et l'état de conformité des environnements existants peut être dégradé.

## Cycle de vie de gestion des secrets

Amazon EVS utilise AWS Secrets Manager pour créer, chiffrer et stocker des secrets dans votre compte lors du déploiement initial de l'environnement. Ces secrets contiennent les informations d'identification VCF nécessaires pour installer et accéder aux dispositifs de gestion VCF tels que vCenter Server, NSX et SDDC Manager, ainsi que le mot de passe racine de l'hôte ESX. Amazon EVS supprime également les secrets gérés en votre nom lorsque l'environnement EVS est supprimé.

Vous êtes responsable de la gestion du cycle de vie secret, y compris de la rotation des secrets. Amazon EVS ne gère pas la rotation de vos secrets. Nous vous recommandons de faire régulièrement pivoter les secrets sur une fenêtre de rotation définie afin de garantir que les secrets ne durent pas longtemps. Pour plus d'informations, consultez la section Programmes de rotation dans le Guide de l'utilisateur de AWS Secrets Manager.

# Création d'un hôte Amazon EVS

Après le déploiement d'un environnement Amazon EVS, vous pouvez ajouter des hôtes pour augmenter la capacité et la résilience de la charge de travail. Amazon EVS prend en charge 4 à 16 hôtes par environnement. Cette action ne peut être utilisée qu'après le déploiement de l'environnement Amazon EVS.

> **Note**
>
> Vous devez attribuer et mettre en service l'hôte dans l'interface utilisateur de SDDC Manager.

Pour créer un hôte Amazon EVS

Suivez ces étapes pour créer un hôte Amazon EVS.

> **Warning**
>
> Les hôtes Amazon EVS utilisent un module complémentaire de fournisseur personnalisé pour fournir des fonctionnalités d'hôte importantes. Lorsque vous ajoutez un hôte à votre environnement, il dispose de la dernière version disponible du module complémentaire personnalisé Amazon EVS. Si votre environnement utilise des hôtes dotés d'une ancienne version du module complémentaire, l'ajout d'un hôte à votre cluster vSphere entraînera l'échec de la correction de l'image du cluster. Pour connaître les étapes à suivre pour résoudre ce problème, consultezthe section called “Résoudre les problèmes liés à l'ajout d'un hôte en raison d'une image de cluster incompatible”.

> **Warning**
>
> Si vous avez mis à jour votre version d'ESX après le déploiement de l'environnement Amazon EVS, le gestionnaire SDDC peut échouer lors de la validation de l'hôte VCF à l'étape des hôtes de commission. Pour connaître les étapes à suivre pour résoudre ce problème, consultezthe section called “Le gestionnaire SDDC échoue à la validation de l'hôte VCF lors de la mise en service de l'hôte”.

> **Note**
>
> Assurez-vous que le nombre d'hôtes Amazon EVS par quota d'environnement EVS est correctement défini pour garantir la réussite de la création d'hôtes. La création d'hôtes échoue si cette valeur de quota est inférieure au nombre d'hôtes que vous essayez de configurer au sein d'un même environnement Amazon EVS. Pour augmenter le quota, vous

pouvez demander une augmentation de quota. Pour de plus amples informations, veuillez consulter Quotas de service.

**Note**

Si vous ne spécifiez pas de version d'ESX lors de l'ajout d'hôtes à votre environnement, Amazon EVS utilise automatiquement la version ESX par défaut associée à la version VCF de votre environnement. Pour plus d'informations, consultez the section called "Versions et EC2 instances VCF".

**Important**

Lorsque vous ajoutez un hôte ESX, sélectionnez une version d'ESX qui correspond à votre cluster vSphere cible. Si la même version n'est pas disponible, déployez une version plus ancienne et mettez-la à niveau à l'aide de vSphere Lifecycle Manager. Pour de plus amples informations, veuillez consulter the section called "Le gestionnaire SDDC échoue à la validation de l'hôte VCF lors de la mise en service de l'hôte". Les mises à niveau peuvent nécessiter le redémarrage de l'hôte et augmenter le temps nécessaire à la mise en service de l'hôte.

Un hôte dont la version d'ESX est plus récente que la version ESX de votre image de cluster vSphere ne peut pas être rétrogradé. Vous devrez supprimer l'hôte et le recréer avec la bonne version d'ESX.

Example

Amazon EVS console and SDDC Managuer UI

1. Accédez à la console Amazon EVS.
2. Dans le volet de navigation, choisissez Environment.
3. Sélectionnez l'environnement dans lequel vous souhaitez créer l'hôte.
4. Sélectionnez l'onglet Hosts.
5. Choisissez Create host (Créer un hôte).
6. Spécifiez les détails de l'hôte et choisissez Create host.

7. Pour vérifier que l'opération est terminée, vérifiez que l'état de l'hôte est passé à Créé.
8. Accédez à SDDC Manager.
9. Mettez en service le nouvel hôte dans SDDC Manager. Pour plus d'informations, consultez Commission Hosts dans la documentation de VMware Cloud Foundation.
10. Ajoutez le nouvel hôte au cluster à l'aide du gestionnaire SDDC. Pour plus d'informations, consultez Comment ajouter un hôte ESX à votre cluster vSphere à l'aide du flux de travail Quickstart dans la documentation de vSphere.

AWS CLI and SDDC Manager UI

1. Ouvrez une nouvelle session de terminal.
2. Créez un nouvel hôte. Voir l'exemple de commande ci-dessous pour référence.

```
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. Accédez à SDDC Manager.
4. Mettez en service le nouvel hôte dans SDDC Manager. Pour plus d'informations, consultez Commission Hosts dans la documentation de VMware Cloud Foundation.
5. Ajoutez le nouvel hôte au cluster à l'aide du gestionnaire SDDC. Pour plus d'informations, consultez Comment ajouter un hôte ESX à votre cluster vSphere à l'aide du flux de travail Quickstart dans la documentation de vSphere.

# Supprimer un hôte Amazon EVS

Vous pouvez supprimer un hôte Amazon EVS de votre environnement lorsqu'il n'est plus nécessaire. Amazon EVS exige que votre environnement dispose d'un minimum de quatre hôtes. Amazon EVS ne prend pas en charge les environnements comportant moins de quatre hôtes.

> **Warning**
>
> La suppression d'un hôte sans le mettre hors service laissera des données périmées dans votre vCenter et votre SDDC Manager, dont le nettoyage peut nécessiter des efforts supplémentaires. Assurez-vous que vos hôtes sont hors service avant de supprimer des hôtes dans la console ou l'API Amazon EVS.

> **Warning**
>
> Utilisez toujours la console ou l'API Amazon EVS pour supprimer vos hôtes Amazon EVS. La suppression d'hôtes de la EC2 console peut laisser votre environnement dans un état incohérent.

Pour supprimer un hôte Amazon EVS

Suivez ces étapes pour supprimer un hôte Amazon EVS.

Example

SDDC Managuer UI and Amazon EVS console

1. Accédez à SDDC Manager.
2. Supprimez le cluster du gestionnaire SDDC.
3. Mettez l'hôte hors service dans SDDC Manager. Pour plus d'informations, consultez la section Démission des hôtes dans la documentation de VMware Cloud Foundation.
4. Accédez à la console Amazon EVS.
5. Dans le volet de navigation, choisissez Environment.
6. Sélectionnez l'environnement qui contient l'hôte à supprimer.
7. Sélectionnez l'onglet Hosts.
8. Choisissez Supprimer l'hôte.
9. Sélectionnez l'hôte et choisissez Supprimer dans l'onglet Hôtes. Répétez cette étape pour chaque hôte que vous souhaitez supprimer.

SDDC Manager UI and AWS CLI

1. Accédez à SDDC Manager.
2. Supprimez le cluster du gestionnaire SDDC.
3. Mettez l'hôte hors service dans SDDC Manager. Pour plus d'informations, consultez la section Démission des hôtes dans la documentation de VMware Cloud Foundation.
4. Ouvrez une nouvelle session de terminal.
5. Supprimez l'hôte. Voir l'exemple de commande ci-dessous pour référence.

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

# La sécurité dans Amazon Elastic VMware Service

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit ceci en tant que sécurité du cloud et sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui s'exécute Services AWS dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de conformitéAWS. Pour en savoir plus sur les programmes de conformité qui s'appliquent à Amazon Elastic VMware Service (Amazon EVS), consultez Services AWS la section Champ d'application par programme de conformité.
- Sécurité dans le cloud — Votre responsabilité est déterminée par Service AWS ce que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation d'Amazon EVS. Il vous explique comment configurer Amazon EVS pour atteindre vos objectifs de sécurité et de conformité. Vous apprendrez également à en utiliser d'autres Services AWS qui vous aident à surveiller et à sécuriser vos ressources Amazon EVS.

Table des matières



## Protection des données dans Amazon EVS

Le modèle de responsabilitéAWS partagée s'applique à la protection des données dans Amazon Elastic VMware Service. Comme décrit dans ce modèle, AWS est responsable de la protection de l'infrastructure mondiale qui gère l'ensemble du AWS cloud. Vous êtes responsable du contrôle de

votre contenu hébergé sur cette infrastructure, y compris les composants VMware Cloud Foundation (VCF). Vous êtes également responsable de la configuration de la sécurité et des tâches de gestion de Services AWS ce que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) relatives à la confidentialité des données. Pour plus d'informations sur la protection des données en Europe, veuillez consulter le billet de blog Modèle de responsabilité partagée AWS et RGPD sur la page Blog Security AWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou Gestion des identités et des accès AWS. Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- SSL/TLS À utiliser pour communiquer avec AWS les ressources. Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour capturer AWS des activités, consultez la section Utilisation des CloudTrail sentiers dans le guide de AWS CloudTrail l'utilisateur.

  > **Note**
  >
  > Amazon EVS n'enregistre pas l'activité des utilisateurs pour les AWS non-composants, tels que l'activité au sein de votre environnement VCF. Ces activités sont enregistrées dans différentes VMware consoles telles que vSphere et NSX Manager. Si une journalisation VCF centralisée est souhaitée, vous pouvez configurer des solutions de surveillance VCF telles que VMware Aria Operations ou VMware Tanzu Observability pour obtenir ce résultat. Pour plus d'informations, consultez VMware Cloud Foundation with VMware Tanzu et VMware Aria Suite Lifecyle en mode VMware Cloud Foundation dans la documentation VCF.

- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels que Amazon Macie, qui aident à découvrir et à sécuriser les données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-3 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS.

Pour plus d'informations sur les points de terminaison FIPS disponibles, consultez Norme FIPS (Federal Information Processing Standard) 140-3.

Nous vous recommandons vivement de ne jamais placer d'informations d'identification sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Nom. Cela inclut lorsque vous travaillez avec Amazon EVS ou une autre entreprise à Services AWS l'aide de la console, de l'API ou AWS SDKs. AWS CLI Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

## Chiffrement au repos

Amazon EVS déploie des EC2 instances i4i.metal qui utilisent le chiffrement AES-256 transparent par défaut pour les données stockées sur le volume de stockage de l'instance. Amazon EVS ne prend pas en charge le chiffrement du volume de démarrage EBS pour le moment.

### Volume de démarrage Amazon EBS

Les instances Amazon EVS i4i.metal utilisent un volume de démarrage Amazon EBS. Le volume de démarrage contient le système d'exploitation et les autres fichiers nécessaires au démarrage et à l'exécution de l' EC2 instance. Le volume de démarrage n'est pas chiffré. Amazon EVS ne prend pas en charge le chiffrement du volume de démarrage pour le moment. Le volume de démarrage ne contient aucune donnée utilisateur provenant de vos machines virtuelles.

### Volume de stockage d'instance

Les EC2 instances Amazon EVS i4i.metal sont fournies avec un stockage NVMe SSD local, qui fait partie du matériel de l'instance. Amazon EVS utilise des volumes de stockage d' NVMe instance comme disques pour les banques de données vSAN. La banque de données vSAN contient vos machines virtuelles de gestion et de charge de travail après le déploiement de votre environnement Amazon EVS.

Les données des volumes de stockage d' NVMe instance sont chiffrées à l'aide d'un chiffrement XTS-AES-256, implémenté sur un module matériel de l'instance. Les clés utilisées pour chiffrer les données écrites sur des périphériques de NVMe stockage connectés localement sont définies par client et par volume. Pour plus d'informations, consultez la section Encryption at rest dans le guide de EC2 l'utilisateur Amazon.

Après avoir déployé l'environnement Amazon EVS, vous pouvez activer le chiffrement data-at-rest vSAN pour toutes les données stockées dans la banque de données vSAN, pour des machines virtuelles individuelles VMs () ou pour des fichiers individuels qu'elles contiennent. VMs Ce contrôle granulaire peut être utile lorsque certains VMs nécessitent un chiffrement alors que d'autres ne le font pas, ou lorsque des disques ou des fichiers spécifiques d'une machine virtuelle doivent être chiffrés. Pour plus d'informations, consultez la section Fonctionnement du Data-At-Rest chiffrement vSAN dans la documentation vSAN VMware .

## Chiffrement en transit

Amazon EVS ne chiffre pas votre trafic en transit par défaut. Pour chiffrer les données en transit qui transitent par Amazon EVS, vous pouvez utiliser le chiffrement de couche application avec un protocole tel que Transport Layer Security (TLS). Pour en savoir plus sur le chiffrement du trafic d' EC2 instance, consultez Encryption in Transit dans le guide de EC2 l'utilisateur Amazon.

> **Note**
>
> Le chiffrement réseau Nitro ne s'applique pas aux EC2 instances déployées par Amazon EVS. Amazon EVS ne prend pas en charge le chiffrement en transit du trafic inter-hôtes.

### Options de chiffrement en transit pour la connectivité sur site

Pour chiffrer le trafic entre votre centre de données sur site et Amazon EVS, vous pouvez combiner l'utilisation de Direct AWS Connect et d' AWS Site-To-Site un VPN avec Transit Gateway AWS . Cette combinaison fournit une IPsec connexion privée cryptée qui réduit également les coûts du réseau, augmente le débit de bande passante et fournit une expérience réseau plus cohérente que les connexions VPN basées sur Internet. Pour plus d'informations, consultez la section AWS Site-to-Site VPN IP privé avec AWS Direct Connect.

> **Note**
>
> Amazon EVS ne prend pas en charge la connectivité via une interface virtuelle privée (VIF) AWS Direct Connect ou via une connexion AWS Site-to-Site VPN qui aboutit directement au VPC sous-jacent. Amazon EVS prend en charge la terminaison du IPSec VPN sur la passerelle NSX Edge de niveau 0 ou de niveau 1. Pour plus d'informations, consultez la section Ajouter un service IPSec VPN NSX dans la documentation de VMware NSX.

MAC Security (MACsec) est une norme IEEE qui garantit la confidentialité, l'intégrité des données et l'authenticité de l'origine des données. Vous pouvez utiliser les connexions AWS Direct Connect qui permettent MACsec de chiffrer vos données entre le centre de données de votre entreprise et le site AWS Direct Connect. Pour plus d'informations, consultez la section Sécurité MAC dans AWS Direct Connect dans le guide de l'utilisateur de AWS Direct Connect.

### Chiffrement en transit pour les données VMware réseau

Une fois l'environnement Amazon EVS déployé, plusieurs options s'offrent à vous pour appliquer le chiffrement des données en transit au niveau de la couche VMware VCF :

- VMware vDefend Distributed Firewall : vous permet de mettre en œuvre une segmentation fine du réseau et d'appliquer le TLS/SSL chiffrement entre les machines virtuelles. Pour plus d'informations, voir Configurer les paramètres de sécurité pour le pare-feu distribué à l'aide de l'interface utilisateur dans la documentation VMware VCF.
- data-in-transitChiffrement vSAN : peut être utilisé pour chiffrer toutes les données et métadonnées entre les hôtes de votre cluster vSAN. Pour plus d'informations, consultez la section Data-In-TransitChiffrement vSAN dans la documentation vSAN VMware .
- vSphere vMotion chiffré : garantit la confidentialité, l'intégrité et l'authenticité des données transférées avec vSphere vMotion. Pour plus d'informations, consultez la section Qu'est-ce que vSphere vMotion crypté dans la documentation de vSphere.

## Gestion des clés et des secrets

Lors du déploiement de l'environnement Amazon EVS, Amazon EVS utilise AWS Secrets Manager pour créer, chiffrer et stocker des secrets contenant les informations d'identification VCF nécessaires pour installer et accéder aux dispositifs de gestion VMware VCF, ainsi que le mot de passe root ESX. Amazon EVS supprime également les secrets gérés en votre nom lorsque l'environnement EVS est supprimé. Pour plus d'informations, consultez la section Contenu d'un secret de Secrets Manager dans le Guide de l'utilisateur de AWS Secrets Manager.

Secrets Manager utilise le chiffrement des enveloppes avec des AWS KMS clés et des clés de données pour protéger chaque valeur secrète. La clé AWS gérée par défaut pour Secrets Manager est utilisée sauf indication contraire. Vous pouvez également spécifier une clé gérée par le client lors de la création de l'environnement pour chiffrer vos secrets. Pour plus d'informations, consultez la section Chiffrement et déchiffrement des AWS secrets dans Secrets Manager dans le guide de l'utilisateur de AWS Secrets Manager.

> **Note**
>
> Des frais d'utilisation supplémentaires s'appliquent aux clés gérées par le client. La clé AWS gérée par défaut est fournie gratuitement. Pour plus d'informations, consultez la section Tarification dans le guide de l'utilisateur de AWS Secrets Manager.

Amazon EVS ne synchronise pas les informations d'identification entre AWS Secrets Manager et votre logiciel VCF après le déploiement. Il vous incombe de vous assurer que les secrets associés à votre environnement Amazon EVS sont synchronisés avec les informations d'identification dans SDDC Manager afin d'éviter l'expiration du mot de passe VCF et la perte d'accès au logiciel VCF.

Amazon EVS n'échange pas les secrets en votre nom. Vous êtes responsable de la rotation des secrets associés à votre environnement. Nous vous recommandons vivement de faire alterner vos secrets dès que l'environnement est créé et de mettre en œuvre un calendrier de rotation pour mettre à jour vos secrets à intervalles réguliers. Pour plus d'informations sur la rotation des AWS secrets de Secrets Manager, consultez la section Rotation by Lambda function dans le guide de l'utilisateur de AWS Secrets Manager. Pour plus d'informations sur la gestion des mots de passe VCF, consultez la section Gestion des mots de passe dans la documentation de VMware Cloud Foundation.

> **Important**
>
> Amazon EVS ne synchronise pas les informations d'identification entre AWS Secrets Manager et votre logiciel VCF après le déploiement. Si vous utilisez AWS Secrets Manager après le déploiement, vous devez synchroniser les informations d'identification entre AWS Secrets Manager et SDDC Manager pour éviter les problèmes d'expiration des mots de passe VCF. Vous risquez de perdre l'accès au logiciel VCF si les informations d'identification du SDDC Manager ne sont pas mises à jour.

> **Note**
>
> Amazon EVS ne propose pas de rotation gérée des secrets.

> **Note**
>
> L'utilisation d'une fonction Lambda pour la rotation des secrets de AWS Secrets Manager entraîne des coûts. Pour plus d'informations, consultez la section Tarification dans le guide de l'utilisateur de AWS Secrets Manager.

## Confidentialité du trafic inter-réseau

Amazon EVS utilise un VPC fourni par le client pour créer des limites entre les ressources de l'environnement Amazon EVS et contrôler le trafic entre celles-ci, votre réseau sur site et Internet. Pour plus d'informations sur Amazon VPC la sécurité, voir Garantir la confidentialité du trafic interréseau Amazon VPC dans le guide de l' Amazon VPC utilisateur.

Par défaut, Amazon EVS crée des sous-réseaux VLAN privés lors de la création de l'environnement qui interdisent l'accès direct à Internet. Pour ajouter un niveau de sécurité supplémentaire à votre VPC, vous pouvez créer une liste de contrôle d'accès réseau personnalisée pour votre VPC avec des règles qui limitent davantage la connectivité Internet. Pour plus d'informations, consultez la section Créer une ACL réseau pour votre VPC dans le guide de l'utilisateur Amazon VPC.

> **Important**
>
> EC2 les groupes de sécurité ne fonctionnent pas sur les interfaces réseau élastiques connectées aux sous-réseaux Amazon EVS VLAN. Pour contrôler le trafic à destination et en provenance des sous-réseaux VLAN Amazon EVS, vous devez utiliser une liste de contrôle d'accès réseau.

Si vous êtes administrateur NSX, vous pouvez configurer les fonctionnalités NSX suivantes pour sécuriser le trafic réseau :

- VMware vDefend Gateway Firewall : sécurise le périmètre du réseau en le protégeant contre les menaces externes (trafic nord-sud). Pour plus d'informations, consultez la section Ajouter une politique et une règle de pare-feu de passerelle dans la documentation de VMware NSX.
- VMware vDefend Distributed Firewall : protège contre les attaques provenant d'un réseau interne (trafic est-ouest). Pour plus d'informations, consultez la section Ajouter un pare-feu distribué dans la documentation de VMware NSX.

# Gestion des identités et des accès pour Amazon Elastic VMware Service

Gestion des identités et des accès AWS (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. IAM les administrateurs contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources Amazon Elastic VMware Service (Amazon EVS). IAM est un Service AWS ventilateur que vous pouvez utiliser sans frais supplémentaires.

Rubriques



## Public ciblé

La façon dont vous utilisez Gestion des identités et des accès AWS (IAM) varie en fonction du travail que vous effectuez dans Amazon EVS.

Utilisateur du service : si vous utilisez le service Amazon EVS pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de plus en plus de fonctionnalités Amazon EVS dans le cadre de votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. Si vous comprenez bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur.

Si vous ne pouvez pas accéder à une fonctionnalité d'Amazon EVS, consultezthe section called "Résolution des problèmes d'identité et d'accès à Amazon EVS".

Administrateur du service : si vous êtes responsable des ressources Amazon EVS au sein de votre entreprise, vous disposez probablement d'un accès complet à Amazon EVS. C'est à vous de déterminer les fonctionnalités et les ressources Amazon EVS auxquelles les utilisateurs de votre

service doivent accéder. Vous devez ensuite envoyer des demandes à votre IAM administrateur pour modifier les autorisations des utilisateurs de votre service. Consultez les informations de cette page pour comprendre les concepts de base de IAM. Pour en savoir plus sur la manière dont votre entreprise peut utiliser IAM Amazon EVS, consultezthe section called "Comment fonctionne Amazon EVS avec IAM".

IAM administrateur - Si vous êtes IAM administrateur, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à Amazon EVS. Pour consulter des exemples de politiques basées sur l'identité Amazon EVS que vous pouvez utiliser dans IAM, consultez. the section called "Exemples de politiques basées sur l'identité Amazon EVS"

## Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur root du AWS compte Utilisateur IAM, ou en assumant un IAM rôle.

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center (IAM Identity Center) les utilisateurs, l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez en tant qu'identité fédérée, votre administrateur a préalablement configuré la fédération d'identité à l'aide de IAM rôles. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez Comment vous connecter à votre Compte AWS compte dans le guide de l'utilisateur de AWS connexion.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, consultez le processus de signature de la version 4 de Signature dans la référence AWS générale.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être également fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en

savoir plus, consultez les sections Authentification multifactorielle du Guide de l'utilisateur d' AWS IAM Identity Center (successeur du Single Sign-On) et Utilisation de l'authentification multifactorielle (MFA) dans AWS le Guide de l'utilisateur IAM. AWS

### AWS utilisateur root du compte

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur root du AWS compte et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur root peut effectuer. Pour obtenir la liste complète des tâches qui nécessitent que vous vous connectiez en tant qu'utilisateur root, consultez la section Tâches nécessitant des informations d'identification d'utilisateur root dans le Guide de référence sur la gestion des comptes.

### Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour plus d'informations sur IAM Identity Center, voir Qu'est-ce qu'IAM Identity Center ? dans le guide de l'utilisateur d' AWS IAM Identity Center (successeur du Single Sign-On). AWS

### Utilisateurs IAM et groupes

An Utilisateur IAMest une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou une seule application. Dans la mesure du possible, nous

vous recommandons de vous fier à des informations d'identification temporaires plutôt que de créer des Utilisateurs IAM personnes possédant des informations d'identification à long terme, telles que des mots de passe et des clés d'accès. Toutefois, si vous avez des cas d'utilisation spécifiques qui nécessitent des informations d'identification à long terme Utilisateurs IAM, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un IAM groupe est une identité qui spécifie une collection de Utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez nommer un groupe IAMAdminset lui donner les autorisations nécessaires pour administrer IAM des ressources.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, consultez la section Quand créer un rôle Utilisateur IAM (au lieu d'un rôle) dans le guide de l'utilisateur IAM.

## IAM rôles

Un IAM rôle est une identité au sein de Compte AWS vous dotée d'autorisations spécifiques. Il est similaire à un Utilisateur IAM, mais n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un IAM rôle dans le en AWS Management Console changeant de rôle. Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez la section Utilisation IAM des rôles dans le Guide de l'utilisateur IAM.

IAM les rôles dotés d'informations d'identification temporaires sont utiles dans les situations suivantes :

- Accès utilisateur fédéré : pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après

leur authentification. Pour plus d'informations sur les ensembles d'autorisations, consultez la section Ensembles d'autorisations du AWS guide de l'utilisateur d'IAM Identity Center (successeur de AWS Single Sign-On).

- Utilisateur IAM Autorisations temporaires — An Utilisateur IAM peut assumer un IAM rôle en assumant temporairement différentes autorisations pour une tâche spécifique.
- Accès entre comptes : vous pouvez utiliser un IAM rôle pour autoriser une personne (un mandant fiable) d'un autre compte à accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour connaître la différence entre les rôles et les politiques basées sur les ressources pour l'accès entre comptes, consultez la section En quoi les IAM rôles diffèrent des politiques basées sur les ressources dans le Guide de l'utilisateur IAM.
- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications Amazon EC2 ou y stocke des objets Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, une fonction du service ou un rôle lié au service.
  - Autorisations principales — Lorsque vous utilisez un rôle Utilisateur IAM ou pour effectuer des actions AWS, vous êtes considéré comme un mandant. Les politiques accordent des autorisations au principal. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui déclenche une autre action dans un autre service. Dans ce cas, vous devez disposer des autorisations nécessaires pour effectuer les deux actions.
  - Rôle de service — Un rôle de service est un IAM rôle qu'un service assume pour effectuer des actions en votre nom. Un IAM administrateur peut créer, modifier et supprimer un rôle de service de l'intérieur IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.
  - Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés au service apparaissent dans votre Compte AWS fichier et appartiennent au service. Un IAM administrateur peut consulter, mais pas modifier les autorisations pour les rôles liés à un service.
- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un IAM rôle pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une Amazon EC2 instance et qui envoient AWS CLI des demandes AWS d'API. Cela est préférable au stockage des clés d'accès dans l' Amazon EC2 instance. Pour attribuer un AWS rôle à une Amazon EC2 instance et le rendre disponible pour toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes exécutés

sur l' Amazon EC2 instance d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez la section Utilisation d'un IAM rôle pour accorder des autorisations aux applications exécutées sur des Amazon EC2 instances dans le Guide de l'utilisateur IAM.

Pour savoir s'il faut utiliser IAM des rôles, consultez la section Quand créer un IAM rôle (au lieu d'un utilisateur) dans le guide de l'utilisateur IAM.

## Gestion de l'accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Chaque IAM entité (utilisateur ou rôle) démarre sans aucune autorisation. Par défaut, les utilisateurs ne peuvent rien faire, pas même changer leur propre mot de passe. Pour autoriser un utilisateur à effectuer une opération, un administrateur doit lui associer une politique d'autorisations. Il peut également ajouter l'utilisateur à un groupe disposant des autorisations prévues. Lorsqu'un administrateur accorde des autorisations à un groupe, tous les utilisateurs de ce groupe se voient octroyer ces autorisations.

IAM les politiques définissent les autorisations pour une action, quelle que soit la méthode que vous utilisez pour effectuer l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

### Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisation JSON que vous pouvez associer à une identité, telle qu'un Utilisateur IAM rôle ou un groupe. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans

quelles conditions. Pour savoir comment créer une politique basée sur l'identité, consultez la section Création de IAM politiques dans le guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

### Politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource telle qu'un Amazon S3 bucket. Les administrateurs de service peuvent utiliser ces stratégies pour définir les actions qu'un principal (membre de compte, utilisateur ou rôle) spécifié peut effectuer sur cette ressource et dans quelles conditions. Les politiques basées sur les ressources sont des politiques en ligne. Il ne s'agit pas de politiques gérées basées sur les ressources.

### Listes de contrôle d'accès (ACLs)

Les listes de contrôle d'accès (ACLs) sont un type de politique qui contrôle les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON. Amazon S3 AWS WAF, et Amazon VPC sont des exemples de services qui soutiennent ACLs. Pour en savoir plus ACLs, consultez la présentation de la liste de contrôle d'accès (ACL) dans le guide du développeur Amazon Simple Storage Service.

### Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limites d'autorisations — Une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une IAM entité (Utilisateur IAM ou à un rôle). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations obtenues représentent la combinaison des politiques basées sur l'identité de l'entité et de ses limites d'autorisations. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites

d'autorisations. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez la section Limites d'autorisations pour les IAM entités dans le guide de l'utilisateur IAM.

- Politiques de contrôle des services (SCPs) : SCPs politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans AWS Organizations. AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer des politiques de contrôle des services (SCPs) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités des comptes membres, y compris pour chaque utilisateur root AWS du compte. Pour plus d'informations sur les Organizations SCPs, voir How SCPs work dans le Guide de l'utilisateur AWS des Organizations.
- Politiques de session : les politiques de session sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une session temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de la session obtenue sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de session. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez Politiques de session dans le Guide de l'utilisateur IAM.

### Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

## Comment fonctionne Amazon EVS avec IAM

Avant de commencer IAM à gérer l'accès à Amazon EVS, découvrez quelles IAM fonctionnalités peuvent être utilisées avec Amazon EVS.

| IAM fonctionnalité | Assistance Amazon EVS |
| --- | --- |
| the section called "Politiques basées sur l'identité pour Amazon EVS" | Oui |

| IAM fonctionnalité | Assistance Amazon EVS |
| --- | --- |
| the section called "Politiques basées sur les ressources au sein d'Amazon EVS" | Non |
| the section called "Actions politiques pour Amazon EVS" | Oui |
| the section called "Ressources relatives aux politiques pour Amazon EVS" | Partielle |
| the section called "Clés de conditions de politique pour Amazon EVS" | Oui |
| the section called "Listes de contrôle d'accès (ACLs) dans Amazon EVS" | Non |
| the section called "Contrôle d'accès basé sur les attributs (ABAC) avec Amazon EVS" | Oui |
| the section called "Utilisation d'informations d'identification temporaires avec Amazon EVS" | Oui |
| the section called "Transférer les sessions d'accès pour Amazon EVS" | Oui |
| the section called "Rôles de service pour Amazon EVS" | Non |
| the section called "Rôles liés à un service pour Amazon EVS" | Oui |

Pour obtenir une vue d'ensemble de la façon dont Amazon EVS et d'autres entreprises Services AWS fonctionnent avec IAM, consultez Services AWS le guide de IAM l'utilisateur d'IAM.

## Politiques basées sur l'identité pour Amazon EVS

Prend en charge les politiques basées sur l'identité : oui

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier les actions et les ressources autorisées ou refusées ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une stratégie basée sur l'identité car il s'applique à l'utilisateur ou au rôle auquel il est attaché. Pour en savoir plus sur tous les éléments que vous utilisez dans une politique JSON, consultez la référence des éléments de stratégie IAM JSON dans le guide de l'utilisateur IAM.

Exemples de politiques basées sur l'identité pour Amazon EVS

Pour consulter des exemples de politiques basées sur l'identité Amazon EVS, consultez. the section called "Exemples de politiques basées sur l'identité Amazon EVS"

Politiques basées sur les ressources au sein d'Amazon EVS

Prend en charge les politiques basées sur les ressources : non

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. L'ajout d'un principal intercompte à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un administrateur IAM du compte sécurisé doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une

politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur d'IAM.

Actions politiques pour Amazon EVS

Soutient les actions Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'`Action`élément d'une politique IAM basée sur l'identité décrit l'action ou les actions spécifiques qui seront autorisées ou refusées par la politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. L'action est utilisée dans une politique pour permettre d'effectuer l'opération associée.

Les actions politiques dans Amazon EVS utilisent le préfixe suivant avant l'action :. `evs:` Par exemple, pour autoriser quelqu'un à créer un environnement avec l'opération d'`CreateEnvironment`API Amazon EVS, vous devez inclure l'`evs:CreateEnvironment`action dans sa politique. Les déclarations de politique doivent inclure un élément `Action` ou `NotAction`. Amazon EVS définit son propre ensemble d'actions décrivant les tâches que vous pouvez effectuer avec ce service.

Pour spécifier plusieurs actions dans une seule déclaration, séparez-les par des virgules comme suit :

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

Vous pouvez aussi spécifier plusieurs actions à l'aide de caractères génériques (*). Par exemple, pour spécifier toutes les actions qui commencent par le mot `List`, incluez l'action suivante :

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

Pour consulter la liste des actions Amazon EVS, consultez la section Actions définies par Amazon EVS dans le Service Authorization Reference.

Ressources relatives aux politiques pour Amazon EVS

Prend en charge les ressources de politique : partiellement

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne prennent pas en charge les autorisations au niveau des ressources, telles que les opérations de listage, utilisez un caractère générique (*) pour indiquer que la déclaration s'applique à toutes les ressources.

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

Pour consulter la liste des types de ressources Amazon EVS et leurs caractéristiques ARNs, consultez la section Ressources définies par Amazon Elastic VMware Service dans le Service Authorization Reference. Pour savoir avec quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par Amazon Elastic VMware Service.

Certaines actions de l'API Amazon EVS prennent en charge plusieurs ressources. Par exemple, plusieurs environnements peuvent être référencés lors de l'appel de l'action `ListEnvironments` API. Pour spécifier plusieurs ressources dans une seule instruction, séparez-les ARNs par des virgules.

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

Par exemple, la ressource d'environnement Amazon EVS possède l'ARN suivant :

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

Pour spécifier les environnements `my-environment-1` et `my-environment-2` dans votre déclaration, utilisez l'exemple suivant ARNs :

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

Pour spécifier tous les environnements appartenant à un compte spécifique, utilisez le caractère générique (*) :

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

Clés de conditions de politique pour Amazon EVS

Prend en charge les clés de condition de politique spécifiques au service : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'`Condition`élément (ou le `Condition` bloc) vous permet de définir les conditions dans lesquelles une instruction est effective. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations de la déclaration ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous ne pouvez accorder Utilisateur IAM l'autorisation d'accéder à une ressource que si elle Utilisateur IAM porte son nom. Pour plus d'informations, consultez IAM la section Éléments de politique : variables et balises dans le guide de l'utilisateur IAM.

Amazon EVS définit son propre ensemble de clés de condition et prend également en charge l'utilisation de certaines clés de condition globales. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Toutes les Amazon EC2 actions prennent en charge les touches de `ec2:Region` condition `aws:RequestedRegion` et. Pour plus d'informations, voir Exemple : restriction de l'accès à une région spécifique.

Pour consulter la liste des clés de condition Amazon EVS, consultez la section Clés de condition pour Amazon EVS dans la référence d'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez Actions définies par Amazon EVS.

## Listes de contrôle d'accès (ACLs) dans Amazon EVS

Supports ACLs : Non

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

## Contrôle d'accès basé sur les attributs (ABAC) avec Amazon EVS

Prise en charge d'ABAC (balises dans les politiques) : Oui

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser les opérations lorsque le tag du principal correspond à celui de la ressource à laquelle il essaie d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

Vous pouvez associer des balises aux ressources Amazon EVS ou transmettre des balises dans une demande adressée à Amazon EVS. Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/<key-name>`, `aws:RequestTag/<key-name>` ou `aws:TagKeys`. Pour plus d'informations sur les actions avec lesquelles vous pouvez utiliser des balises dans les clés de condition, consultez la section Actions définies par Amazon EVS dans le Service Authorization Reference.

## Utilisation d'informations d'identification temporaires avec Amazon EVS

Prend en charge les informations d'identification temporaires : oui

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent

avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation d'IAM dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez Passage d'un rôle utilisateur à un rôle IAM (console) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM.

## Transférer les sessions d'accès pour Amazon EVS

Prend en charge les sessions d'accès direct (FAS) : oui

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transfert des sessions d'accès.

## Rôles de service pour Amazon EVS

Prend en charge les rôles de service : Non

Un rôle de service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

### Rôles liés à un service pour Amazon EVS

Prend en charge les rôles liés à un service : oui

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour en savoir plus sur la création ou la gestion des rôles liés aux services Amazon EVS, consultez. the section called "Utilisation des rôles liés à un service"

## Exemples de politiques basées sur l'identité Amazon EVS

Par défaut, Utilisateurs IAM les rôles ne sont pas autorisés à créer ou à modifier des ressources Amazon EVS. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l' AWS API AWS Management Console AWS CLI, ou. Un IAM administrateur doit créer des IAM politiques qui accordent aux utilisateurs et aux rôles l'autorisation d'effectuer des opérations d'API spécifiques sur les ressources spécifiques dont ils ont besoin. L'administrateur doit ensuite associer ces politiques au Utilisateurs IAM ou aux groupes qui nécessitent ces autorisations.

Pour savoir comment créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de stratégie JSON, consultez la section Création de politiques à l'aide de l'éditeur JSON dans le guide de l'utilisateur IAM.

Rubriques



### Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer des ressources Amazon EVS dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Appliquer les autorisations du moindre privilège : lorsque vous définissez des autorisations à IAM l'aide de politiques, accordez uniquement les autorisations nécessaires à l'exécution d'une tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation IAM pour appliquer des autorisations, consultez la section Politiques et autorisations IAM dans le guide de l'utilisateur IAM.
- Utilisez des conditions dans IAM les politiques pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques pour limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que CloudFormation. Pour plus d'informations, consultez la section Éléments de politique IAM JSON : condition dans le guide de l'utilisateur IAM.
- IAM Access Analyzer À utiliser pour valider vos IAM politiques afin de garantir des autorisations sécurisées et fonctionnelles : IAM Access Analyzer valide les politiques nouvelles et existantes afin qu'elles respectent le langage des politiques (JSON) et les IAM meilleures pratiques. IAM IAM Access Analyzer fournit plus de 100 vérifications des politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez la section Validation des IAM Access Analyzer politiques dans le guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui Utilisateurs IAM nécessite ou root des utilisateurs sur votre compte, activez l'authentification MFA pour plus de sécurité. Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Configuration de l'accès aux API protégé par MFA dans le Guide de l'utilisateur IAM.

## Utilisation de la console Amazon EVS

Pour accéder à la console Amazon EVS, un principal IAM doit disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent permettre au principal de répertorier et de consulter les informations relatives aux ressources Amazon EVS de votre Compte AWS compte. Si vous créez une politique basée sur l'identité qui est plus restrictive que les autorisations minimales requises, la console ne fonctionnera pas comme prévu pour les principaux auxquels cette politique est associée.

Pour vous assurer que vos principaux IAM peuvent toujours utiliser la console Amazon EVS, créez une politique avec votre propre nom unique, par exemple. `AmazonEVSAdminPolicy` Attachez la politique aux principaux. Pour plus d'informations, veuillez consulter Ajout d'autorisations à un utilisateur dans le Guide de l'utilisateur 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"
                }
            }
        }
    ]
}
```

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l’accès uniquement aux actions qui correspondent à l’opération API que vous essayez d’effectuer.

## Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment vous pouvez créer une politique qui Utilisateurs IAM permet de visualiser les politiques intégrées et gérées associées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or 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": "*"
        }
    ]
```

```
}
```

## Création et gestion d'un environnement Amazon EVS

Cet exemple de politique inclut les autorisations requises pour créer et supprimer un environnement Amazon EVS, ainsi que pour ajouter ou supprimer des hôtes une fois l'environnement créé.

Vous pouvez le Région AWS remplacer par Région AWS celui dans lequel vous souhaitez créer un environnement. Si votre compte possède déjà le rôle `AWSServiceRoleForAmazonEVS`, vous pouvez supprimer l'action `iam:CreateServiceLinkedRole` de la politique. Si vous avez déjà créé un environnement Amazon EVS dans votre compte, un rôle doté de ces autorisations existe déjà, sauf si vous l'avez supprimé.

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

## Obtenez et listez les environnements Amazon EVS, les hôtes et VLANs

Cet exemple de politique inclut les autorisations minimales requises pour qu'un administrateur puisse obtenir et répertorier tous les environnements Amazon EVS, les hôtes et VLANs au sein d'un compte donné dans le Région AWS us-east-2.

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

```
      ],
      "Resource": "*"
    }
  ]
}
```

# Résolution des problèmes d'identité et d'accès à Amazon EVS

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Amazon EVS et IAM.

Rubriques

- AccessDeniedException
- Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder à mes ressources Amazon EVS

## AccessDeniedException

Si vous recevez un message `AccessDeniedException` lors de l'appel d'une opération d' AWS API, cela signifie que les informations d'identification principales IAM que vous utilisez ne disposent pas des autorisations requises pour effectuer cet appel.

```
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
```

Dans l'exemple de message précédent, l'utilisateur n'est pas autorisé à appeler l'opération d'`CreateEnvironment`API Amazon EVS. Pour fournir des autorisations d'administrateur Amazon EVS à un directeur IAM, consultez. the section called “Exemples de politiques basées sur l'identité Amazon EVS”

Pour des informations plus générales sur IAM, consultez la section Contrôler l'accès aux AWS ressources à l'aide de politiques dans le Guide de l'utilisateur IAM.

## Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder à mes ressources Amazon EVS

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez

spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACLs), vous pouvez utiliser ces politiques pour autoriser les utilisateurs à accéder à vos ressources.

Pour plus d'informations, consultez les éléments suivants :

- Pour savoir si Amazon EVS prend en charge ces fonctionnalités, consultezthe section called "Comment fonctionne Amazon EVS avec IAM".
- Pour savoir comment fournir l'accès à vos ressources sur un site Comptes AWS qui vous appartient, consultez la section Fournir un accès à un Utilisateur IAM autre Compte AWS que vous possédez dans le Guide de l'utilisateur d'IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Octroi d'accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour connaître la différence entre l'utilisation de rôles et de politiques basées sur les ressources pour l'accès entre comptes, consultez la section En quoi les IAM rôles diffèrent des politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

## AWS politiques gérées pour Amazon EVS

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle Service

AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants. Pour plus d'informations, consultez la section Politiques AWS gérées dans le Guide de IAM l'utilisateur.

## AWS politique gérée : Amazon EVSService RolePolicy

Vous ne pouvez pas associer `AmazonEVSServiceRolePolicy` à vos entités IAM. Cette politique est associée à un rôle lié à un service qui permet à Amazon EVS d'effectuer des actions en votre nom. Pour de plus amples informations, veuillez consulter the section called "Utilisation des rôles liés à un service". Lorsque vous créez un environnement à l'aide d'un principal IAM `iam:CreateServiceLinkedRole` autorisé, le rôle `AWSServiceRoleforAmazonEVS` lié au service est automatiquement créé pour vous avec cette politique qui y est attachée.

Cette politique autorise le rôle `AWSServiceRoleForAmazonEVS` lié au service à appeler en votre Services AWS nom.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes qui permettent à Amazon EVS d'effectuer les tâches suivantes.

- `ec2`- Découvrez les composants du réseau VPC, notamment les sous-réseaux et. VPCs Créez, modifiez, balisez et supprimez des interfaces réseau élastiques utilisées pour établir une connexion permanente entre Amazon EVS et l'appliance VMware Virtual Cloud Foundation (VCF) SDDC Manager dans votre sous-réseau VPC. Cette connectivité est requise pour qu'Amazon EVS puisse déployer, gérer et surveiller le déploiement du VCF.
- `ec2`- Supprimez les instances EC2 créées par Amazon EVS lorsque vous faites une demande de suppression d'hôte EVS. Décrivez et modifiez les attributs de l'instance EC2 afin que la protection par défaut contre l'arrêt et l'arrêt de l'instance EC2 puisse être désactivée si nécessaire pour prendre en charge la suppression de l'hôte EVS.
- `ec2`- Gérez les volumes EBS pour l'installation et le nettoyage de Cloud Builder. Lors de la création de l'environnement, Cloud Builder est installé sur l'un des hôtes déployés par Amazon EVS pour effectuer des modifications de configuration VCF. Une fois l'opération terminée, Amazon EVS supprime Cloud Builder en détachant et en supprimant le volume EC2 sur lequel il est stocké.
- `ec2`- Supprimez les sous-réseaux VLAN EVS en votre nom si vous demandez la suppression de l'environnement.
- `secretsmanager`- Supprimez les mots de passe VCF qu'Amazon EVS crée et stocke dans AWS Secrets Manager lors de la création de l'environnement. Amazon EVS supprime tous les

secrets créés par le service dans votre compte si la création de l'environnement échoue ou si vous demandez la suppression de l'environnement. Récupérez les informations d'identification de vCenter auprès de AWS Secrets Manager lorsque vous configurez un connecteur vCenter en fournissant un ARN secret. L'autorisation est assortie d'une condition de balise de ressource afin de garantir qu'Amazon EVS accède uniquement `EvsAccess=true` aux secrets explicitement étiquetés pour l'accès à Amazon EVS vCenter.

- `kms`- Déchiffrez les secrets et décrivez les clés KMS lorsque les informations d'identification de vCenter stockées dans Secrets Manager sont chiffrées à l'aide de clés KMS. L'autorisation est assortie d'une condition de balise de ressource afin de garantir qu'Amazon EVS accède uniquement `EvsAccess=true` aux clés KMS explicitement étiquetées pour l'accès à vCenter.
- `cloudwatch`- Publiez des statistiques AWS d'utilisation CloudWatch pour les ressources Amazon EVS dotées de quotas.

Pour en savoir plus sur la politique, y compris la dernière version du document de politique JSON, consultez Amazon EVSService RolePolicy dans le  AWS Managed Policy Reference Guide.

## Amazon EVS met à jour les politiques AWS gérées

Consultez les informations relatives aux mises à jour des politiques AWS gérées pour Amazon EVS depuis que ce service a commencé à suivre ces modifications. Pour obtenir des alertes automatiques sur les modifications apportées à cette page, abonnez-vous au flux RSS de la page Historique de la documentation.

| Modifier | Description | Date |
| --- | --- | --- |
| Amazon EVSService RolePolicy — Politique mise à jour | Amazon EVS a mis à jour la politique pour permettre au service de récupérer les informations d'identification vCenter auprès de Secrets AWS Manager et de déchiffre r les secrets chiffrés à l'aide de clés KMS. Pour en savoir plus, veuillez consulter la section the section called “AWS | 23 mars 2026 |

| Modifier | Description | Date |
| --- | --- | --- |
| | politique gérée : Amazon EVSService RolePolicy". | |
| Amazon EVSService RolePolicy — Politique mise à jour | Amazon EVS a mis à jour la politique afin d'ajouter des fonctionnalités complètes de gestion des ressources, notamment la gestion des instances EC2, les opérations de volume EBS et l'intégration de AWS Secrets Manager. Pour en savoir plus, veuillez consulter la section the section called "AWS politique gérée : Amazon EVSService RolePolicy". | 14 août 2025 |
| Amazon EVSService RolePolicy — Politique mise à jour | Amazon EVS a mis à jour la politique pour permettre au service de supprimer les sous-réseaux VLAN EVS, ainsi que de publier les métriques d'utilisation d'Amazon EVS sur. CloudWatch Pour en savoir plus, veuillez consulter la section the section called "AWS politique gérée : Amazon EVSService RolePolicy". | 14 juillet 2025 |

| Modifier | Description | Date |
| --- | --- | --- |
| Amazon EVSService RolePolicy — Ajout d'une nouvelle politique | Amazon EVS a ajouté une nouvelle politique qui permet au service de se connecter à un sous-réseau VPC dans le compte client. Cette connexion est requise pour le fonctionnement du service. Pour en savoir plus, veuillez consulter la section the section called "AWS politique gérée : Amazon EVSService RolePolicy". | 9 juin 2025 |
| Amazon EVS a commencé à suivre les modifications | Amazon EVS a commencé à suivre les modifications apportées à ses politiques AWS gérées. | 9 juin 2025 |

## Utilisation de rôles liés à un service pour Amazon EVS

Amazon Elastic VMware Service utilise des AWS rôles liés au service Identity and Access Management (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à Amazon EVS. Les rôles liés à un service sont prédéfinis par Amazon EVS et incluent toutes les autorisations requises par le service pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service facilite la configuration d'Amazon EVS, car vous n'avez pas à ajouter manuellement les autorisations nécessaires. Amazon EVS définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul Amazon EVS peut assumer ses rôles. Les autorisations définies comprennent la politique de confiance et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Cela protège vos ressources Amazon EVS, car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès aux ressources.

Pour plus d'informations sur les autres services prenant en charge les rôles liés à un service, consultez les services AWS opérationnels avec IAM et recherchez les services présentant la mention Yes (Oui) dans la colonne Service-linked roles (Rôles liés à un service). Choisissez un Oui ayant un lien permettant de consulter les détails du rôle pour ce service.

## Autorisations de rôle liées à un service pour Amazon EVS

Amazon EVS utilise le rôle lié au service nommé. `AWSServiceRoleForAmazonEVS` Ce rôle permet à Amazon EVS de gérer les environnements de votre compte. La politique ci-jointe permet au rôle de gérer les ressources suivantes : interfaces réseau EVS Elastic, sous-réseaux VLAN EVS, hôtes EVS et métriques. VPCs CloudWatch

Le rôle lié à un service `AWSServiceRoleForAmazonEVS` approuve les services suivants pour endosser le rôle :

- `evs.amazonaws.com`

La politique d'autorisation des rôles permet à Amazon EVS d'effectuer les actions suivantes sur les ressources spécifiées :

- AmazonEVSServiceRolePolicy

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

## Création d'un rôle lié à un service pour Amazon EVS

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous créez un environnement dans la AWS Management Console AWS CLI ou l' AWS API, Amazon EVS crée le rôle lié au service pour vous.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous créez un environnement, Amazon EVS crée à nouveau le rôle lié au service pour vous.

## Modification d'un rôle lié à un service pour Amazon EVS

Amazon EVS ne vous permet pas de modifier le rôle lié au `AWSServiceRoleForAmazonEVS` service. Après avoir créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car

plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez Modification d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

### Supprimer un rôle lié à un service pour Amazon EVS

Si vous n'avez plus besoin d'utiliser une fonctionnalité ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Cependant, vous devez nettoyer votre rôle lié à un service avant de pouvoir le supprimer manuellement.

Nettoyage d'un rôle lié à un service

Avant de pouvoir utiliser IAM pour supprimer un rôle lié à un service, vous devez supprimer toutes les ressources utilisées par le rôle. Pour savoir comment supprimer un environnement Amazon EVS avec des hôtes, consultezthe section called "Supprimer les hôtes et l'environnement Amazon EVS".

> **Note**
>
> Si le service Amazon EVS utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

Suppression manuelle du rôle lié au service

Utilisez la console IAM, la AWS CLI ou l' AWS API pour supprimer le rôle lié au `AWSServiceRoleForAmazonEVS` service. Pour plus d'informations, consultez la section Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

### Régions prises en charge pour les rôles liés au service Amazon EVS

Amazon EVS prend en charge l'utilisation de rôles liés au service dans toutes les régions où le service est disponible. Pour plus d'informations, consultez la section Points de terminaison et quotas Amazon Elastic VMware Service dans le Guide de référence AWS général.

## Résilience dans Amazon EVS

L'infrastructure AWS mondiale est construite autour Régions AWS de zones de disponibilité. Régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées,

connectées via un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Les environnements Amazon EVS sont disponibles dans une seule zone de AWS disponibilité. Pour garantir la haute disponibilité de l'infrastructure mono-AZ Amazon EVS, Amazon EVS propose les fonctionnalités suivantes :

> **Note**
>
> Amazon EVS prend uniquement en charge les déploiements mono-AZ pour le moment.

- Amazon EVS prend en charge l'utilisation d' AWS Elastic Disaster Recovery pour automatiser la sauvegarde et la restauration de vos données.
- Amazon EVS déploie un cluster Active/Standby NSX Edge avec deux nœuds NSX Edge conformément aux exigences du VCF. Les nœuds NSX Edge s'exécutent sur différents hôtes afin de garantir une haute disponibilité et de permettre un basculement rapide en cas de défaillance d'un nœud NSX Edge.
- Amazon EVS déploie un environnement minimal de quatre hôtes ESX, ce qui est requis par VCF. Des hôtes supplémentaires peuvent être ajoutés après le déploiement. Il s'agit d'une exigence de VMware conception visant à garantir un quorum vSAN approprié et à maintenir la disponibilité pendant les opérations de maintenance et les défaillances de l'hôte. Pour plus d'informations, consultez la section vSphere Cluster Design for VMware Cloud Foundation dans la documentation de VMware Cloud Foundation.
- Amazon EVS prend en charge l'utilisation d'un groupe de placement de EC2 partitions ou d'un groupe de placement de clusters pour les EC2 hôtes. Le groupe de placement de partitions répartit vos EC2 instances sur des partitions logiques de telle sorte que les groupes d'instances d'une partition ne partagent pas le matériel sous-jacent avec des groupes d'instances situés dans différentes partitions. Cette stratégie permet de réduire le risque de défaillances matérielles corrélées pour les charges de travail distribuées importantes. Les groupes de placement en cluster sont utilisés pour placer vos EC2 instances dans le même rack physique afin de garantir une faible latence. Pour plus d'informations, consultez la section Groupes de placement de partitions dans le Guide de Amazon EC2 l'utilisateur.

Pour plus d'informations sur AWS les régions et les zones de disponibilité, consultez la section Infrastructure AWS mondiale.

## VMware résilience des composants

Les clients Amazon EVS sont chargés de configurer les VMware composants exécutés sur Amazon EVS afin de garantir la haute disponibilité de vos machines virtuelles (VMs) et la résilience de la charge de travail.

Amazon EVS prend en charge les fonctionnalités de résilience VMware Cloud Foundation (VCF) suivantes :

- vSphere Replication : fournit une réplication asynchrone basée sur l'hôte à des fins de reprise après sinistre et de migration de charge VMs de travail. Pour plus d'informations, consultez la section Fonctionnement de vSphere Replication dans la documentation de VMware vSphere Replication.
- Protection des données vSAN : vous permet de récupérer rapidement après une défaillance opérationnelle due à des attaques VMs de ransomware, à l'aide de snapshots natifs stockés localement sur le cluster vSAN. Pour plus d'informations, consultez la section Utilisation de la protection des données vSAN dans la documentation vSAN.
- vSphere HA : fournit un basculement automatique VMs en cas de défaillance de l'hôte. Pour plus d'informations, consultez la section Conception de haute disponibilité pour vCenter Server for VMware Cloud Foundation dans la documentation VCF.
- vSphere Fault Tolerance (FT) : assure une disponibilité continue pour les applications critiques VMs en créant et en gérant une autre machine virtuelle identique et disponible en permanence pour la remplacer en cas de basculement. Pour plus d'informations, consultez la section Fonctionnement de la tolérance aux pannes dans la documentation de vSphere.
- VSAN Failure to Tolerate (FTT) : paramètre vSAN qui détermine le nombre de défaillances d'hôte auxquelles une machine virtuelle peut résister avant de devenir inaccessible. Cela définit le niveau de redondance et de tolérance aux pannes de vos machines virtuelles au sein du cluster vSAN. Pour plus d'informations, consultez Tolérer des défaillances supplémentaires avec un domaine de défaillance dans un cluster vSAN dans la documentation vSAN.

# Utilisation d'Amazon EVS avec d'autres services AWS

Amazon EVS est intégré à d'autres Services AWS pour fournir des solutions supplémentaires. Cette rubrique décrit certains des services avec lesquels Amazon EVS travaille pour ajouter des fonctionnalités.

Rubriques



# Créez des ressources Amazon EVS avec AWS CloudFormation

Amazon EVS est intégré à AWS CloudFormation un service qui vous aide à modéliser et à configurer vos AWS ressources afin que vous puissiez passer moins de temps à créer et à gérer vos ressources et votre infrastructure. Vous créez un modèle qui décrit toutes les AWS ressources que vous souhaitez, un environnement Amazon EVS par exemple, et vous vous AWS CloudFormation occupez du provisionnement et de la configuration de ces ressources pour vous.

Lorsque vous l'utilisez AWS CloudFormation, vous pouvez réutiliser votre modèle pour configurer vos ressources Amazon EVS de manière cohérente et répétée. Décrivez simplement vos ressources une seule fois, puis fournissez les mêmes ressources encore et encore dans plusieurs Comptes AWS régions.

## Amazon EVS et modèles AWS CloudFormation

Pour fournir et configurer des ressources pour Amazon EVS et les services associés, vous devez comprendre les AWS CloudFormation modèles. Les modèles sont des fichiers texte formatés en JSON ou YAML. Ces modèles décrivent les ressources que vous souhaitez mettre à disposition dans vos AWS CloudFormation piles. Si vous n'êtes pas familiarisé avec JSON ou YAML, vous pouvez utiliser AWS CloudFormation Designer pour vous aider à démarrer avec les AWS CloudFormation modèles. Pour plus d'informations, voir Qu'est-ce que AWS CloudFormation Designer ? dans le guide de AWS CloudFormation l'utilisateur.

Amazon EVS prend en charge la création d'environnements dans. AWS CloudFormation Pour plus d'informations, notamment des exemples de modèles JSON et YAML pour vos environnements, consultez la référence des types de ressources Amazon EVS dans le guide de l' AWS CloudFormation utilisateur.

## En savoir plus sur AWS CloudFormation

Pour en savoir plus AWS CloudFormation, consultez les ressources suivantes :

- AWS CloudFormation
- AWS CloudFormation Guide de l'utilisateur
- AWS CloudFormation Guide de l'utilisateur de l'interface de ligne de commande

# Exécutez des charges de travail à hautes performances avec Amazon FSx pour ONTAP NetApp

Amazon FSx for NetApp ONTAP est un service de stockage qui vous permet de lancer et d'exécuter des systèmes de fichiers ONTAP entièrement gérés dans le cloud. ONTAP NetApp est une technologie de système de fichiers qui fournit un ensemble largement adopté de fonctionnalités d'accès et de gestion des données. FSx for ONTAP fournit les fonctionnalités, les performances et les systèmes APIs de NetApp fichiers sur site avec l'agilité, l'évolutivité et la simplicité d'un service entièrement géré. AWS Pour plus d'informations, consultez le guide de FSx l'utilisateur d'ONTAP.

Amazon EVS prend en charge l'utilisation d'Amazon FSx for NetApp ONTAP en tant que NFS/iSCSI banque de données et en tant que stockage connecté aux clients pour les VMware machines virtuelles exécutées sur Amazon EVS.

## Configuration FSx pour NetApp ONTAP en tant que banque de données NFS

La procédure suivante détaille les étapes minimales requises FSx pour configurer NetApp ONTAP en tant que banque de données NFS pour Amazon EVS à l'aide de la console FSx et de l'interface client VMware vSphere qui s'exécute sur Amazon EVS.

### Conditions préalables

Avant d'utiliser Amazon EVS avec Amazon FSx for NetApp ONTAP, assurez-vous que les tâches préalables suivantes ont été effectuées.

- Un environnement Amazon EVS est déployé dans votre Virtual Private Cloud (VPC). Pour de plus amples informations, veuillez consulter Prise en main.
- Vous avez accès à votre client vSphere exécuté sur Amazon EVS.

- Vous ou votre administrateur de stockage devez disposer des autorisations nécessaires pour créer et gérer les FSx systèmes de fichiers ONTAP dans votre VPC. Pour plus d'informations, consultez la section Gestion des identités et des accès pour Amazon FSx pour NetApp ONTAP.

Votre principal IAM dispose des autorisations appropriées pour créer et gérer les FSx systèmes de fichiers ONTAP dans votre VPC. Pour de plus amples informations, veuillez consulter the section called "Création et gestion d'un environnement Amazon EVS".

## Création d'un système FSx de fichiers pour NetApp ONTAP

1. Accédez à la FSx console Amazon.
2. Choisissez Create file system (Créer un système de fichiers).
3. Sélectionnez Amazon FSx pour NetApp ONTAP.
4. Choisissez Suivant.
5. Sélectionnez Création standard.
6. Pour Type de déploiement, sélectionnez une option de déploiement mono-AZ.

> **Note**
>
> Amazon EVS prend uniquement en charge les déploiements mono-AZ pour le moment.

7. Pour la capacité de stockage SSD, spécifiez 1024 GiB.
8. Pour Capacité de débit, choisissez Spécifier la capacité de débit. Choisissez au moins 512 MB/s pour Single-AZ 1 ou au moins 768 MB/s pour Single-AZ 2.
9. Sélectionnez le VPC Amazon EVS connecté à vos sous-réseaux Amazon EVS VLAN.
10. Sélectionnez un groupe de sécurité qui autorise tout le trafic NFS ONTAP requis FSx vers le sous-réseau VLAN de VMkernel gestion des hôtes Amazon EVS.
11. Sélectionnez le sous-réseau d'accès au service Amazon EVS dans lequel votre système de fichiers sera déployé. Pour de plus amples informations, veuillez consulter the section called "Sous-réseau d'accès au service".
12. Pour Junction path, spécifiez un nom significatif permettant `/vol1` d'identifier ce volume dans vSphere.
13. Dans Configuration du volume par défaut, définissez l'efficacité du stockage sur Activé.
14. Conservez les valeurs par défaut des autres paramètres et choisissez Next.
15. Passez en revue les attributs du système de fichiers et choisissez Créer un système de fichiers.

### Récupérez le nom DNS NFS de la machine virtuelle de stockage

1. Accédez à la FSx console Amazon.
2. Dans le menu de gauche, sélectionnez Systèmes de fichiers.
3. Choisissez le système de fichiers nouvellement créé.
4. Sélectionnez l'onglet Machines virtuelles de stockage.
5. Choisissez la machine virtuelle de stockage.
6. Sélectionnez l'onglet Endpoints.
7. Copiez le nom DNS du système de fichiers réseau (NFS) pour une utilisation ultérieure dans VMware Vsphere.

### Créez une banque de données NFS dans vSphere à l'aide du volume for ONTAP FSx

Suivez les instructions de la section Créer une banque de données NFS dans un environnement vSphere pour configurer Amazon FSx for NetApp ONTAP en tant que stockage externe pour vSphere. VMware Pour le réglage du serveur dans l'interface client vSphere, utilisez le nom DNS NFS de la machine virtuelle de stockage (SVM) que vous avez copié à l'étape précédente.

## Configuration FSx pour NetApp ONTAP en FSx tant que banque de données iSCSI

La procédure suivante détaille les étapes minimales requises FSx pour configurer NetApp ONTAP en tant que banque de données iSCSI pour Amazon EVS à l'aide de FSx la console VMware et de l'interface client vSphere qui s'exécute sur Amazon EVS.

### Conditions préalables

Avant d'utiliser Amazon EVS avec Amazon FSx for NetApp ONTAP, assurez-vous que les tâches préalables suivantes ont été effectuées.

- Un environnement Amazon EVS est déployé dans votre Virtual Private Cloud (VPC). Pour de plus amples informations, veuillez consulter Prise en main.
- Vous avez accès à votre client vSphere exécuté sur Amazon EVS.
- Vous ou votre administrateur de stockage devez disposer des autorisations nécessaires pour créer et gérer les FSx systèmes de fichiers ONTAP dans votre VPC. Pour plus d'informations, consultez Gestion des identités et des accès pour Amazon FSx pour NetApp ONTAP.

## Création d'un système FSx de fichiers pour NetApp ONTAP

1. Accédez à la FSx console Amazon.
2. Choisissez Create file system (Créer un système de fichiers).
3. Sélectionnez Amazon FSx pour NetApp ONTAP.
4. Choisissez Suivant.
5. Sélectionnez Création standard.
6. Pour Type de déploiement, sélectionnez une option de déploiement mono-AZ.

> **Note**
>
> Amazon EVS prend uniquement en charge les déploiements mono-AZ pour le moment.

7. Pour la capacité de stockage SSD, spécifiez 1024 GiB.
8. Pour Capacité de débit, choisissez Spécifier la capacité de débit. Choisissez au moins 512 MB/s pour Single-AZ 1 ou au moins 768 MB/s pour Single-AZ 2.
9. Sélectionnez le VPC Amazon EVS connecté à vos sous-réseaux Amazon EVS VLAN.
10. Sélectionnez un groupe de sécurité qui autorise tout le trafic iSCSI ONTAP requis FSx vers le sous-réseau VLAN de gestion des VMkernel hôtes Amazon EVS.
11. Sélectionnez le sous-réseau d'accès au service Amazon EVS dans lequel votre système de fichiers sera déployé. Pour de plus amples informations, veuillez consulter the section called "Sous-réseau d'accès au service".
12. Dans Configuration du volume par défaut, définissez l'efficacité du stockage sur Activé.
13. Conservez les valeurs par défaut des autres paramètres et choisissez Next.
14. Vérifiez les attributs du système de fichiers et choisissez Créer un système de fichiers.

## Configuration d'un adaptateur iSCSI logiciel dans vSphere pour le stockage d'hôtes ESX

Pour chaque hôte ESX, vous devez configurer l'adaptateur iSCSI logiciel afin que vos hôtes ESX puissent l'utiliser pour accéder au stockage iSCSI. Pour obtenir des instructions sur la configuration de l'adaptateur logiciel iSCSI pour les hôtes ESX dans vSphere, reportez-vous à la section Ajouter ou supprimer l'adaptateur logiciel iSCSI dans la documentation du produit vSphere. VMware

Après avoir configuré l'adaptateur iSCSI logiciel, copiez le nom qualifié iSCSI (IQN) associé à un adaptateur iSCSI. Ces valeurs seront utilisées ultérieurement.

## Création d'un LUN iSCSI

FSx for ONTAP vous permet de créer des numéros d'unité logique (LUNs) spécifiquement destinés à l'accès iSCSI, fournissant ainsi un stockage par blocs partagé à vos hôtes ESX. Vous utilisez la CLI NetApp ONTAP pour créer un LUN.

Vous trouverez ci-dessous un exemple de commande.

> **Note**
>
> Il est recommandé de configurer la taille du LUN à 90 % de la taille du volume.

```
lun create -vserver <your_svm_name> \
-path /vol/<your_volume_name>/<lun_name> \
-size <required_datastore_capacity> \
-ostype vmware
```

Pour plus d'informations, consultez la section Création d'un LUN iSCSI dans le guide de l'utilisateur FSx pour ONTAP.

## Configuration et mappage d'un groupe d'initiateurs sur le LUN iSCSI

Maintenant que vous avez créé un LUN iSCSI, l'étape suivante du processus consiste à créer un groupe d'initiateurs (`igroup`) pour connecter le volume au cluster et mapper le LUN au groupe d'initiateurs. Vous utilisez la CLI NetApp ONTAP pour effectuer ces actions.

1. Configurez le groupe d'initiateurs.

   Vous trouverez ci-dessous un exemple de commande. Pour `--initiator` ce faire, utilisez l'adaptateur iSCSI IQNs que vous avez copié à l'étape précédente.

   ```
   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. Confirmez qu'`igroup`il existe.

```
lun igroup show
```

3. Mappez le LUN au groupe d'initiateurs. Vous trouverez ci-dessous un exemple de commande.

```
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. Utilisez la `lun show -path` commande pour vérifier que le LUN est créé, en ligne et mappé.

```
lun show -path /vol/<vol_name>/<lun_name> -fields state,mapped,serial-hex
```

Pour plus d'informations, consultez la section Provisioning iSCSI pour Linux ou Provisioning iSCSI pour Windows dans FSx le guide de l'utilisateur pour ONTAP.

## Configuration de la découverte dynamique du LUN iSCSI dans vSphere

Pour permettre aux hôtes ESX de voir le LUN iSCSI, vous devez configurer la découverte dynamique pour chaque hôte dans l'interface client vSphere. Dans le champ du serveur iSCSI, entrez le nom DNS (NFS) que vous avez copié à l'étape précédente. Pour plus d'informations, consultez la section Configurer la découverte dynamique ou statique pour iSCSI et iSER sur ESX Host dans la documentation du produit vSphere VMware .

## Création d'une banque de données VMFS dans VMware vSphere à l'aide du LUN iSCSI

Les banques de données VMFS (Virtual Machine File System) servent de référentiels pour les machines virtuelles. VMware Suivez les instructions de la section Créer une banque de données vSphere VMFS pour configurer la banque de données VMFS dans VMware vSphere à l'aide du LUN iSCSI que vous avez précédemment configuré.

# Résolution des problèmes

Ce chapitre détaille certains problèmes courants rencontrés lors de la création ou de la gestion des environnements Amazon EVS.

# Résoudre les problèmes liés aux échecs des vérifications de l'état de

Amazon EVS effectue des contrôles automatisés de votre environnement afin d’identifier les problèmes. Vous pouvez consulter le statut de votre environnement pour identifier des problèmes spécifiques et détectables.

## Consulter les informations de vérification de l'état de l'environnement

Pour étudier les environnements altérés à l'aide de la console Amazon EVS

1. Ouvrez la console Amazon EVS.
2. Dans le volet de navigation, choisissez Environments, puis sélectionnez votre environnement.
3. Sélectionnez l'onglet Détails pour obtenir une vue d'ensemble de l'environnement.
4. Vérifiez l'état de l'environnement. Passez le pointeur de la souris sur ce champ pour afficher une fenêtre contextuelle contenant des résultats individuels pour chaque vérification de l'état de l'environnement.

## Le contrôle d'accessibilité a échoué

Le contrôle d'accessibilité vérifie qu'Amazon EVS dispose d'une connexion permanente à SDDC Manager. Si Amazon EVS ne parvient pas à accéder à l’environnement, cette vérification échoue.

Dans ce cas, Amazon EVS ne peut plus accéder à SDDC Manager pour vérifier le statut de l’environnement, et l’ajout d’hôtes à ce dernier n’est plus possible. L’échec au test d’accessibilité entraîne également l’échec des vérifications de réutilisation des clés de licence et de couverture des clés, et la vérification du nombre d’hôtes renvoie la réponse Inconnu.

Pour garantir l'accessibilité, vérifiez les points suivants :

- Assurez-vous que vos certificats sont valides et qu’ils n’ont pas expiré. Vous pouvez utiliser l’interface utilisateur de SDDC Manager ou le client vSphere pour gérer les certificats d’un

environnement VCF. Après le déploiement, il est recommandé de remplacer tous les certificats du domaine de gestion VMware Cloud Foundation. Pour plus d'informations, consultez la section Gestion des certificats dans VMware Cloud Foundation dans la documentation de VMware Cloud Foundation.

- Assurez-vous que vos serveurs DNS sont accessibles depuis le sous-réseau d'accès aux services, que les enregistrements DNS sont valides et qu'il n'existe aucun nom d'hôte ou adresse IP dupliqué.
- Si vous souhaitez créer vos propres règles de pare-feu, suivez ces instructions :
  - TCP/UDP Autorisez l'accès aux serveurs DNS.
  - Autorisez HTTPS/SSH l'accès au sous-réseau VLAN de gestion de l'hôte.
  - Autorisez HTTPS/SSH l'accès au sous-réseau VLAN de la machine virtuelle de gestion.

Si vous ne parvenez toujours pas à résoudre le problème après avoir suivi ces instructions, nous vous recommandons de contacter le AWS Support pour obtenir une assistance supplémentaire.

## Echec de la vérification du nombre d'hôtes

Cette vérification permet de vérifier que votre environnement possède un minimum de quatre hôtes, ce qui est une exigence pour VCF 5.2.x.

Si ce contrôle échoue, vous devez ajouter des hôtes pour que votre environnement atteigne cette exigence minimale. Amazon EVS prend uniquement en charge les environnements comprenant entre 4 et 16 hôtes.

## Échec de la vérification de réutilisation des clés

Cette vérification permet de vérifier que la clé de licence VCF n'est pas utilisée par un autre environnement Amazon EVS. Les licences VCF ne peuvent être utilisées que par un seul environnement Amazon EVS. Cette vérification échoue si vous fournissez des clés de licence VCF dans une demande de création d'environnement qui sont déjà utilisées par un autre environnement.

Le cas échéant, vous obtenez une réponse d'erreur indiquant que l'environnement Amazon EVS n'a pas pu être créé. Pour résoudre le problème, vérifiez les paramètres de votre licence dans SDDC Manager et remplacez toutes les licences précédemment utilisées par des licences inutilisées.

> **Important**
>
> Utilisez l'interface utilisateur du SDDC Manager pour gérer la solution VCF et les clés de licence vSAN. Amazon EVS exige que vous conserviez des clés de solution VCF et de licence vSAN valides dans SDDC Manager pour que le service fonctionne correctement. Bien que les clés doivent être attribuées à vos hôtes et à votre cluster vSAN à l'aide de vSphere Client, vous devez vous assurer que ces clés apparaissent également dans l'écran de licence de l'interface utilisateur de SDDC Manager.

## La vérification de la couverture des clés a échoué

Ce contrôle vérifie que votre clé de licence VCF attribuée à vCenter Server alloue suffisamment de cœurs vCPU et de capacité de stockage vSAN (Tio) à tous les hôtes déployés.

Le cas échéant, vous obtenez une réponse d'erreur indiquant que l'environnement Amazon EVS n'a pas pu être créé. Un échec au test de couverture des clés peut indiquer l'un des problèmes suivants :

- Les licences VCF ne sont pas correctement attribuées à vCenter Server. Vous devez attribuer une licence à vCenter Server avant l'expiration de sa période d'évaluation ou de la licence en cours. Si tel est le problème, passez en revue les attributions de licences dans SDDC Manager.
- Les licences VCF actuelles ne couvrent pas les besoins en matière de cœur de vCPU et de capacité de stockage vSAN. La clé de solution VCF doit comporter au moins 256 cœurs. La clé de licence vSAN doit avoir au moins 110 TiB de capacité vSAN. Le cas échéant, ajoutez des licences vSAN dans SDDC Manager jusqu'à ce que vos besoins en matière d'utilisation soient satisfaits.

Si les actions ci-dessus ne permettent pas de résoudre le problème, contactez le AWS Support pour obtenir de l'aide.

> **Important**
>
> Utilisez l'interface utilisateur du SDDC Manager pour gérer la solution VCF et les clés de licence vSAN. Amazon EVS exige que vous conserviez des clés de solution VCF et de licence vSAN valides dans SDDC Manager pour que le service fonctionne correctement. Bien que les clés doivent être attribuées à vos hôtes et à votre cluster vSAN à l'aide de vSphere Client, vous devez vous assurer que ces clés apparaissent également dans l'écran de licence de l'interface utilisateur de SDDC Manager.

# L'agent vSphere HA sur cet hôte n'a pas pu atteindre l'adresse d'isolement

Dans l'interface utilisateur de vCenter, lorsque l'hôte ESX est sélectionné, le message « L'agent vSphere HA sur cet hôte n'a pas pu atteindre l'adresse d'isolation < adresse> » s'affiche. IPv6

Ce message d'erreur indique que l'agent vSphere HA sur un hôte n'est pas en mesure d'atteindre l'adresse d' IPv6 isolation par défaut utilisée par vSphere HA pour les tests de pulsation. Le message d'erreur n'indique aucun problème et se produit uniquement parce qu'Amazon EVS n'est pas pris en charge pour le IPv6 moment. L'absence de IPV6 support pour Amazon EVS n'affecte pas les fonctionnalités de base de vSphere HA.

# Les prévérifications de mise à niveau de vSAN échouent pour le cluster hôte ESX

Lorsque vous tentez de mettre à niveau le cluster hôte ESX à l'aide de SDDC Manager, les prévérifications relatives au disque vSAN peuvent échouer. Cela est dû au fait qu'Amazon EVS utilise l'architecture de stockage vSAN Express (ESA) et que les vérifications préalables à la mise à niveau ne s'appliquent pas à vSAN ESA. Pour plus d'informations, consultez l'article de la base de connaissances Broadcom à ce sujet.

# Ajouter une défaillance de l'hôte due à une image de cluster incompatible

Problème

Lorsque vous ajoutez un hôte à votre environnement, celui-ci dispose de la dernière version disponible du module complémentaire EVS Custom Vendor. Si votre environnement utilise des hôtes dotés d'une ancienne version du module complémentaire, l'ajout de nouveaux hôtes échoue avec un message d'erreur indiquant que le nouvel hôte n'est pas compatible avec votre image de cluster. Pour résoudre ce problème, vous devez utiliser vSphere Lifecyle Manager pour extraire la dernière version du module complémentaire disponible de l'hôte récemment ajouté.

Solution

Procédez comme suit :

1. Accédez à l'inventaire des hôtes et des clusters dans VMware vCenter Server.
2. Extrayez le module complémentaire de l'hôte récemment ajouté en créant un cluster vide temporaire.
3. Sous Notions de base, sélectionnez Importer une image depuis un hôte existant dans le vCenter Inventory et créez le cluster. Conservez tous les autres paramètres par défaut.
4. Une fois ce cluster temporaire créé avec l'image extraite, vous pouvez le supprimer. Le module complémentaire sera désormais disponible dans votre dépôt vSphere Lifecycle Manager.
5. Accédez à votre cluster d'environnement et sélectionnez l'onglet Mises à jour.
6. Modifiez l'image de votre cluster et remplacez la version du module complémentaire par la version récemment extraite.
7. Choisissez Enregistrer.
8. Dans le gestionnaire SDDC, réessayez la tâche d'ajout d'hôte qui a échoué. Cela corrigera les hôtes de votre cluster, en mettant à jour tous les hôtes avec la dernière version du module complémentaire. La correction de l'image du cluster nécessitera le redémarrage de l'hôte.

## Le gestionnaire SDDC échoue à la validation de l'hôte VCF lors de la mise en service de l'hôte

Problème

Si vous avez mis à jour votre version d'ESX après le déploiement de l'environnement Amazon EVS, le gestionnaire SDDC peut échouer lors de la validation de l'hôte VCF à l'étape des hôtes de commission. Pour résoudre ce problème, vous devrez utiliser vSphere Lifecyle Manager pour mettre à niveau ESX sur le nouvel hôte.

Solution

Procédez comme suit :

> **Important**
>
> Ces étapes nécessitent l'ajout temporaire de l'hôte à vCenter en dehors de SDDC Manager. L'utilisation de vSphere Lifecyle Manager pour des opérations autres que les mises à niveau d'ESX peut rendre votre hôte inutilisable et vous obliger à supprimer et à créer un nouvel hôte Amazon EVS.

1. Accédez à l'inventaire des hôtes et des clusters dans VMware vCenter Server.
2. Ajoutez temporairement l'hôte à votre centre de données virtuel, en veillant à sélectionner Gérer l'hôte avec une image. L'hôte sera supprimé ultérieurement une fois la mise à niveau d'ESX terminée. Pour plus d'informations, consultez Comment ajouter un hôte à votre centre de données ou à votre dossier vSphere dans la documentation de vSphere.
3. Une fois l'hôte ajouté à vSphere, mettez à niveau la version ESX sur l'hôte. Cela peut être fait dans l'onglet Mises à jour de votre hébergeur. Modifiez l'image de l'hôte pour qu'elle corresponde à la version ESX de votre cluster.
4. Une fois la mise à niveau terminée, supprimez l'hôte de votre inventaire vCenter. Pour plus d'informations, consultez la section Comment supprimer un hôte ESX de votre instance de vCenter Server dans la documentation de vSphere.
5. Inscrivez votre hôte dans le gestionnaire SDDC. Pour plus d'informations, consultez Commission Hosts dans la documentation de VMware Cloud Foundation.
6. Une fois l'hôte mis en service, ajoutez-le à votre cluster à l'aide de SDDC Manager.

# Journalisation des appels d'API Amazon EVS à l'aide de AWS CloudTrail

Amazon EVS est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur IAM, un rôle IAM ou un service AWS dans Amazon EVS. CloudTrail capture tous les appels AWS d'API pour Amazon EVS sous forme d'événements. Les appels capturés incluent des appels provenant de la console Amazon EVS et des appels de code vers les opérations de l'API Amazon EVS. Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour Amazon EVS. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été envoyée à Amazon EVS, l'adresse IP à partir de laquelle la demande a été faite, l'auteur de la demande, la date à laquelle elle a été faite, ainsi que des informations supplémentaires.

Pour en savoir plus CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

> **Note**
>
> Amazon EVS n'enregistre pas l'activité des utilisateurs pour les AWS non-composants, tels que l'activité au sein de votre environnement VCF. Ces activités sont enregistrées dans différentes VMware consoles telles que vSphere et NSX Manager.
> Si vous souhaitez une journalisation VCF centralisée, vous pouvez configurer des solutions de surveillance VCF telles que VMware Cloud Foundation Operations pour obtenir ce résultat.

## Informations Amazon EVS dans CloudTrail

CloudTrail est activé sur votre AWS compte lorsque vous le créez. Lorsqu'une activité se produit dans Amazon EVS, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre AWS compte. Pour plus d'informations, consultez la section Affichage des événements à l'aide de l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de votre AWS compte, y compris des événements pour Amazon EVS, créez un historique. Un suivi permet CloudTrail de fournir des fichiers journaux

à un compartiment Amazon S3. Par défaut, lorsque vous créez un parcours dans la console, celui-ci s'applique à toutes les AWS régions. Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- Présentation de la création d'un journal de suivi
- CloudTrail services et intégrations pris en charge
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux provenant de plusieurs régions
- Réception de fichiers CloudTrail journaux provenant de plusieurs comptes

Toutes les actions Amazon EVS sont enregistrées CloudTrail et documentées dans le manuel Amazon EVS API Reference. Par exemple, les appels au`CreateEnvironment`, `GetEnvironment` et les `DeleteEnvironment` actions génèrent des entrées dans les fichiers CloudTrail journaux.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été faite avec les informations d'identification root ou AWS celles de l'utilisateur Identity and Access Management (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la demande a été faite par un autre AWS service.

Pour de plus amples informations, veuillez consulter l'élément userIdentity CloudTrail .

## Comprendre les entrées du fichier journal Amazon EVS

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent

pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

# Quotas de service Amazon EVS

Amazon EVS a intégré Service Quotas, Service AWS qui vous permet de consulter et de gérer vos quotas depuis un emplacement central. Pour plus d'informations, veuillez consulter Qu'est-ce que Service Quotas? dans le Guide de l'utilisateur Service Quotas.

Grâce à l'intégration des Quotas de Service, vous pouvez utiliser le AWS Management Console ou AWS CLI pour rechercher la valeur de vos quotas Amazon EVS et demander une augmentation de quota pour des quotas ajustables. Pour plus d'informations, consultez la section Demande d'augmentation de quota dans le Guide de l'utilisateur du Service Quotas et request-service-quota-increasedans le Guide de référence des AWS CLI commandes.

Pour plus d'informations sur les quotas de service Amazon EVS, consultez la section Quotas Amazon EVS dans le Guide de référence AWS général.

**Important**

Assurez-vous que votre quota d'instances standard d' EC2 exécution à la demande reflète le nombre de v CPUs dont vous avez besoin pour toutes les EC2 instances que vous utiliserez sur Amazon EVS. Chaque instance d'i4i.metal utilise 128 v. CPUs Pour plus d'informations sur l'augmentation des quotas de EC2 service, consultez la section Demander une augmentation dans le guide de EC2 l'utilisateur Amazon.

**Note**

Si vous prévoyez d'utiliser des hôtes EC2 dédiés pour votre environnement Amazon EVS, assurez-vous que votre quota d'hôtes EC2 dédiés i4i reflète le nombre d'hôtes dédiés que vous avez l'intention d'utiliser pour la région souhaitée. Pour plus d'informations sur l'augmentation des quotas de EC2 service, consultez la section Demander une augmentation dans le guide de EC2 l'utilisateur Amazon.

> **Note**
>
> Si vous configurez la connectivité Internet HCX, votre quota IPAM pour la longueur du masque de réseau IPv4 CIDR public contigu fourni par Amazon doit être de /28 ou plus. Pour plus d'informations, consultez la section Quotas pour votre IPAM.

> **Note**
>
> Amazon CloudWatch collecte des statistiques AWS d'utilisation pour les ressources Amazon EVS soumises à des quotas (environnement et hôtes). Pour plus d'informations, consultez la section Mesures CloudWatch d'utilisation dans le guide de CloudWatch l'utilisateur Amazon.

# Consultez les quotas de service Amazon EVS dans le AWS Management Console

1. Ouvrez la console Service Quotas.
2. Dans le volet de navigation de gauche, sélectionnez  AWS services.
3. Dans la liste des  AWS services, recherchez et sélectionnez Amazon Elastic VMware Service.
4. Choisissez Afficher les quotas.

   Dans la liste des quotas de service, vous pouvez voir le nom du quota de service, la valeur appliquée (si elle est disponible), le quota AWS par défaut et si la valeur du quota est ajustable.
5. Pour afficher des informations supplémentaires sur un quota de service, notamment la description, choisissez le nom du quota.
6. (Facultatif) Pour demander une augmentation de quota, sélectionnez le quota que vous souhaitez augmenter, sélectionnez Demander une augmentation au niveau du compte, entrez ou sélectionnez les informations requises, puis sélectionnez Demander.

Pour mieux utiliser les quotas de service à l'aide du AWS Management Console, consultez le Guide de l'utilisateur des quotas de service. Pour demander une augmentation de quota, consultez Demander une augmentation de quota dans le Guide de l'utilisateur de Service Quotas.

# Afficher les quotas de service Amazon EVS avec la CLI AWS

Exécutez la commande suivante pour afficher vos quotas 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**
>
> Le quota renvoyé est le nombre d'environnements ou d'hôtes Amazon EVS qui peuvent être créés dans ce compte dans la AWS région actuelle.

Pour travailler davantage avec les quotas de service à l'aide de la AWS CLI, consultez service-quotas dans le manuel de référence des commandes de la AWS CLI. Pour demander une augmentation du quota, consultez la request-service-quota-increasecommande dans le manuel de référence des commandes de la AWS CLI.

# Historique du document pour le guide de l'utilisateur d'Amazon Elastic VMware Service

Le tableau suivant décrit les versions de documentation pour Amazon Elastic VMware Service.

| Modification | Description | Date |
| --- | --- | --- |
| Amazon mis à jour EVSServic e RolePolicy | Amazon EVS a mis à jour la politique gérée `AmazonEVS ServiceRolePolicy` pour permettre au service de récupérer les informations d'identification vCenter auprès de Secrets AWS Manager et de déchiffrer les secrets chiffrés à l'aide de clés KMS gérées par le client. | 23 mars 2026 |
| Amazon mis à jour EVSServic e RolePolicy | Amazon EVS a mis à jour la politique gérée `AmazonEVS ServiceRolePolicy` pour ajouter des fonctionn alités complètes de gestion des ressources, notamment la gestion des instances EC2, les opérations de volume EBS et l'intégration de AWS Secrets Manager. Pour plus d'informa tions, consultez les mises à jour des politiques AWS gérées par Amazon EVS. | 14 août 2025 |
| Amazon mis à jour EVSServic e RolePolicy | Mise à jour de la politique AWS gérée Amazon EVSServiceRolePolicy. | 4 août 2025 |

| | | |
|---|---|---|
| Publication du nombre d'environnements par quota de AWS compte | Amazon EVS a publié le nombre d'environnements par quota de AWS compte.<br><br>Le nombre d'environnements par quota de AWS compte représente le nombre maximum d'environnements Amazon EVS pouvant être créés dans un compte et une région donnés. | 8 juillet 2025 |
| Amazon EVS est disponible dans la région Europe (Irlande) | Amazon EVS a été lancé dans la région Europe (Irlande). | 18 juin 2025 |
| A publié Amazon EVSService RolePolicy | La politique AWS gérée Amazon EVSService RolePolicy a été publiée. | 9 juin 2025 |
| Publication initiale du guide de l'utilisateur | Le guide de l'utilisateur d'Amazon Elastic VMware Service a été publié.<br><br>Le guide de l'utilisateur Amazon EVS décrit tous les concepts d'Amazon EVS et fournit des instructions sur l'utilisation des différentes fonctionnalités à la fois avec la console et l'interface de ligne de commande. | 9 juin 2025 |

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.