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 ? ... 1
Caractéristiques d'Amazon EVS ... 1
Commencez à utiliser Amazon EVS ... 2
Accès à Amazon EVS ... 2
Concepts et composants ... 3
Environnement Amazon EVS ... 3
Hôte Amazon EVS ... 3
Sous-réseau d'accès aux services ... 3
Sous-réseau VLAN Amazon EVS ... 4
VMware NSX ... 6
VMware Extension de cloud hybride (HCX) ... 6
Architecture ... 6
Topologie du réseau ... 8
Ressources Amazon EVS ... 11
Configuration d'Amazon Elastic VMware Service ... 13
Inscrivez-vous pour AWS ... 13
Créer un utilisateur IAM ... 14
Création d'un rôle IAM pour déléguer l'autorisation Amazon EVS à un utilisateur IAM ... 15
Souscrivez à un AWS plan Business, AWS Enterprise On-Ramp ou AWS Enterprise Support ... 18
Vérifiez les quotas ... 18
Planifier les tailles de CIDR VPC ... 18
Création d'une réservation Amazon EC2 Capacity ... 19
Configurez le AWS CLI ... 19
Création d'une paire de Amazon EC2 clés ... 19
Préparez votre environnement pour VMware Cloud Foundation (VCF) ... 20
Acquérir des clés de licence VCF ... 20
VMware Prérequis HCX ... 20
Premiers pas ... 22
Prérequis ... 23
Création d'un VPC avec des sous-réseaux et des tables de routage ... 23
Configurer les serveurs DNS et NTP à l'aide du jeu d'options DHCP VPC ... 25
Configuration du serveur DNS ... 26
Configuration du serveur NTP ... 27

(Facultatif) Configurer la connectivité réseau sur site à l'aide AWS Direct Connect d' AWS Site-to-Site un VPN avec AWS Transit Gateway ... 28
Configuration d'une instance de serveur de routage VPC avec des points de terminaison et des homologues ... 28
Création d'un environnement Amazon EVS ... 30
Vérifier la création de l'environnement Amazon EVS ... 42
Associer des sous-réseaux VLAN Amazon EVS à une table de routage ... 44
Créez une ACL réseau pour contrôler le trafic du sous-réseau Amazon EVS VLAN ... 45
Récupérez les informations d'identification VCF et accédez aux appareils de gestion VCF ... 45
Configuration de la console EC2 série ... 46
Connect à la console EC2 série ... 46
Configuration de l'accès à la console EC2 série ... 47
Nettoyage ... 47
Supprimer les hôtes et l'environnement Amazon EVS ... 47
Supprimer les composants du serveur de routage VPC ... 50
Supprimer la liste de contrôle d'accès réseau (ACL) ... 50
Supprimer les interfaces réseau élastiques ... 51
Dissocier et supprimer les tables de routage des sous-réseaux ... 51
Supprimer des sous-réseaux ... 51
Supprimer le VPC ... 51
Étapes suivantes ... 51
Migration ... 52
Prérequis ... 52
Vérifiez l'état du sous-réseau VLAN HCX ... 53
Vérifiez que le sous-réseau VLAN HCX est associé à une ACL réseau ... 54
Créez un groupe de ports distribués avec l'ID VLAN de liaison montante publique HCX ... 55
(Facultatif) Configurer l'optimisation du réseau WAN HCX ... 55
(Facultatif) Activer le réseau optimisé pour la mobilité HCX ... 56
Vérifiez la connectivité HCX ... 56
Sécurité ... 57
Gestion des identités et des accès ... 58
Public ciblé ... 58
Authentification par des identités ... 59
Gestion des accès à l'aide de politiques ... 63
Comment fonctionne Amazon Elastic VMware Service avec IAM ... 66
Exemples de politiques basées sur l'identité Amazon EVS ... 74

Résolution des problèmes d'identité et d'accès à Amazon Elastic VMware Service 87
AWS politiques gérées 88
Utilisation des rôles liés à un service 90
Utilisation avec d'autres services 94
AWS CloudFormation 94
Amazon EVS et modèles AWS CloudFormation 94
En savoir plus sur AWS CloudFormation 95
Amazon FSx pour NetApp ONTAP 95
Configuration en tant que banque de données NFS 96
Configuration en tant que banque de données iSCSI 98
Résolution des problèmes 102
Résoudre les problèmes liés aux échecs des vérifications de l'état de 102
Consulter les informations de vérification de l'état de l'environnement 102
Le contrôle d'accessibilité a échoué 102
Echec de la vérification du nombre d'hôtes 103
Échec de la vérification de réutilisation des clés 103
La vérification de la couverture des clés a échoué 104
L'agent vSphere HA sur cet hôte n'a pas pu atteindre l'adresse d'isolement 105
Points de terminaison et quotas 106
Points de terminaison de service 106
Quotas de service 107
Historique de la documentation 109
..... cx

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

> **Note**
>
> Amazon EVS est en version préliminaire publique et est sujet à modification.

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
- Commencez à utiliser Amazon EVS
- Accès à Amazon EVS
- Concepts et composants d'Amazon EVS
- Architecture Amazon EVS

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 celles-ci.

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, consultezPremiers pas. 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

> **Note**
>
> Amazon EVS est en version préliminaire publique et est sujet à modification.

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 VMware ESXi hôte qui s'exécute sur des instances Amazon EC2 bare metal.

Sous-réseau d'accès aux services

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 appareils et hôtes VCF. ESXi 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. Les sous-réseaux VLAN Amazon EVS ont une taille de bloc CIDR minimale de /28 et une taille maximale de /24. 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. Pour de plus amples informations, veuillez consulter the section called “Considérations relatives à la mise en 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**
>
> EC2 les règles des groupes de sécurité 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.

> **Note**
>
> Amazon EVS n'est pas pris en charge pour le IPv6 moment.

Sous-réseau VLAN VMkernel de gestion de l'hôte

Le sous-réseau VLAN de VMkernel 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. ESXi

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. ESXi

Sous-réseau VLAN de gestion des machines virtuelles

Le sous-réseau VLAN de gestion des machines virtuelles 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 NSX Edge actifs/en veille, 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 AWS 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

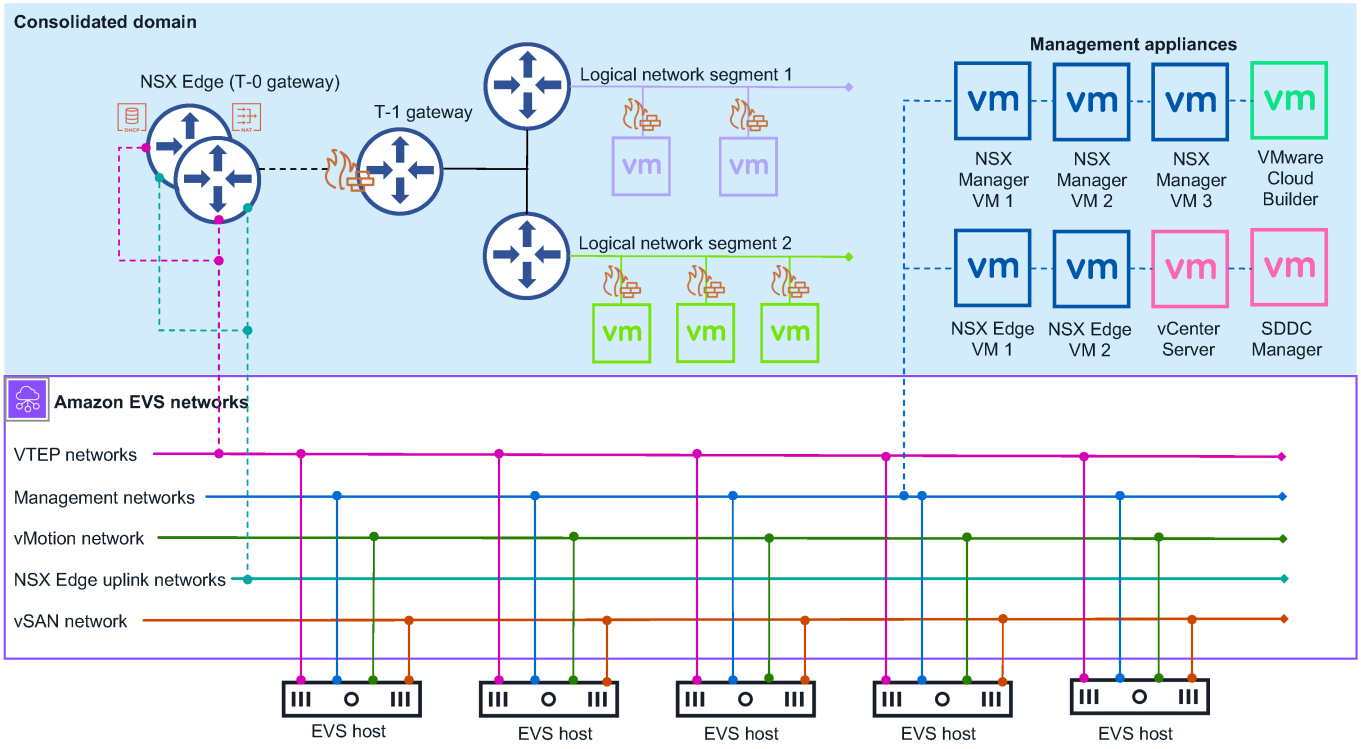
> **Note**
>
> Amazon EVS est en version préliminaire publique et est sujet à modification.

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 :

- ESXi hôtes
- 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 NSX Edge actif/en veille 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 NSX Edge actif/en veille 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 AWS Direct Connect l'aide AWS Site-to-Site d'un VPN avec une passerelle de transit.

Considérations relatives à la mise en 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 plus d'informations, voir sous-réseau d'accès aux services.

> **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 du serveur 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 sous-réseaux VLAN Amazon EVS ont une taille de bloc CIDR minimale de /28 et une taille maximale de /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 NSX Edge actif/en veille 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 actif/veille. 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.
- ESXi Hôtes Amazon EVS 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

> **Note**
>
> Amazon EVS est en version préliminaire publique et est sujet à modification.

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).

Rubriques

- Inscrivez-vous pour AWS
- Créer un utilisateur IAM
- Création d'un rôle IAM pour déléguer l'autorisation Amazon EVS à un utilisateur IAM
- Souscrivez à un AWS plan Business, AWS Enterprise On-Ramp ou AWS Enterprise Support
- Vérifiez les quotas
- Planifier les tailles de CIDR VPC
- Création d'une réservation Amazon EC2 Capacity
- Configurez le AWS CLI
- Création d'une paire de Amazon EC2 clés
- Préparez votre environnement pour VMware Cloud Foundation (VCF)
- Acquérir des clés de licence VCF
- VMware Prérequis HCX

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 IAM console (Console IAM) en tant que propriétaire du compte en choisissant Root user (Utilisateur racine) et en entrant l'adresse e-mail de votre compte AWS. 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. Activez la case à cocher en regard de l'accès à AWS Management Console. Ensuite, sélectionnez Custom password (Mot de passe personnalisé), puis saisissez votre nouveau mot de passe dans la zone de texte.
5. Par défaut, AWS oblige le nouvel utilisateur à 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 Filter policies (Filtrer les stratégies), puis sélectionnez AWS managed -job function (Fonction professionnelle gérée par AWS) pour filtrer le contenu de la table.
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 de l'utilisateur et du rôle IAM à la facturation avant de pouvoir utiliser les autorisations `AdministratorAccess` 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 d'autres groupes et utilisateurs et pour accorder l'accès aux ressources de votre compte AWS à vos utilisateurs. Pour en savoir plus sur l'utilisation de politiques qui limitent les autorisations des utilisateurs à des ressources AWS spécifiques, consultez Gestion des accès et exemples de politiques.

Création d'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' AWS Identity and Access Management 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 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 possède la valeur de quota minimale requise au niveau du compte de 4 pour le nombre d'hôtes par quota d'environnement EVS. La valeur par défaut est 0. Pour de plus amples informations, veuillez consulter the section called “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

Pour permettre la création d'un environnement Amazon EVS, vous devez fournir à Amazon EVS un VPC contenant un sous-réseau et suffisamment d'espace d'adresse IP pour qu'Amazon EVS puisse créer les sous-réseaux VLAN qui se connectent à vos appareils VCF. Pour plus d'informations,

consultez the section called "Considérations relatives à la mise en réseau Amazon EVS" et the section called "Sous-réseau VLAN Amazon EVS".

Création d'une réservation Amazon EC2 Capacity

Amazon EVS lance des instances Amazon EC2 i4i.metal qui représentent ESXi les hôtes de 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 la version 5.2.1 de la version VCF. Pour plus d'informations, consultez les notes de mise à jour de VCF 5.2.1

> **Note**
>
> Amazon EVS prend uniquement en charge la version 5.2.1.x de VCF pour le moment.

Acquérir des 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.

> **Note**
>
> 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. Si vous gérez ces clés à l'aide de vSphere Client, vous devez vous assurer qu'elles apparaissent également dans l'écran de licence de l'interface utilisateur de SDDC Manager.

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.

- 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.
- VMware NSX est installé et configuré dans votre environnement. Pour plus d'informations, consultez le guide d'installation de VMware NSX.
- VMware HCX est activé et installé dans votre environnement. Pour plus d'informations, consultez À propos de la mise en route avec VMware HCX dans le guide de démarrage avec VMware HCX.

Commencer à utiliser Amazon Elastic VMware Service

> **Note**
>
> Amazon EVS est en version préliminaire publique et est sujet à modification.

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 la version 5.2.1 de la version VCF. Pour plus d'informations, consultez les notes de mise à jour de VCF 5.2.1.

> **Important**
>
> Amazon EVS prend uniquement en charge la version 5.2.1.x de VCF pour le moment.

Rubriques

- Prérequis
- Création d'un VPC avec des sous-réseaux et des tables de routage
- Configurer les serveurs DNS et NTP à l'aide du jeu d'options DHCP VPC
- (Facultatif) Configurer la connectivité réseau sur site à l'aide AWS Direct Connect d' AWS Site-to-Site un VPN avec AWS Transit Gateway

- Configuration d'une instance de serveur de routage VPC avec des points de terminaison et des homologues
- Création d'un environnement Amazon EVS
- Vérifier la création de l'environnement Amazon EVS
- Associer des sous-réseaux VLAN Amazon EVS à une table de routage
- Créez une ACL réseau pour contrôler le trafic du sous-réseau Amazon EVS VLAN
- Récupérez les informations d'identification VCF et accédez aux appareils de gestion VCF
- Configuration de la console EC2 série
- Nettoyage
- Étapes suivantes

Prérequis

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.

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. Les sous-réseaux Amazon EVS ont une taille de bloc CIDR minimale de /28

et une taille maximale de /24. Pour de plus amples informations, consultez the section called "Considérations relatives à la mise en réseau Amazon EVS".

> **Note**
>
> Amazon EVS n'est pas pris en charge 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, consultezPoints de terminaison et quotas.

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.
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. Les sous-réseaux VPC doivent avoir une taille de bloc CIDR minimale de /28. Les sous-réseaux VLAN Amazon EVS ont une taille de bloc CIDR minimale de /28 et une taille maximale de /24.

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**
>
> Amazon VPC crée automatiquement une table de routage principale et y associe des sous-réseaux par défaut. Amazon EVS créera des sous-réseaux dans la table de routage principale.

Configurer les serveurs DNS et NTP à l'aide du jeu d'options DHCP VPC

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

- Serveurs DNS (Domain Name System) utilisés pour résoudre les adresses IP des hôtes.
- Serveurs NTP (Network Time Protocol) utilisés pour éviter les problèmes de synchronisation horaire dans le SDDC.

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 du serveur DNS

Vous pouvez saisir IPv4 les adresses d'un maximum de quatre serveurs DNS (Domain Name System). Vous pouvez l'utiliser Route 53 comme fournisseur de serveur DNS ou vous pouvez fournir vos propres serveurs DNS personnalisés. Pour plus d'informations sur la configuration de Route 53 en tant que service DNS pour un domaine existant, consultez Faire de Route 53 le service DNS d'un domaine en cours d'utilisation.

> **Note**
>
> L'utilisation à la fois de Route 53 et d'un serveur DNS (Domain Name System) personnalisé peut entraîner un comportement inattendu.

> **Note**
>
> Amazon EVS n'est pas pris en charge pour le IPv6 moment.

Pour déployer correctement un environnement, 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, comme indiqué dans. the section called "Création d'un environnement Amazon EVS"

- Une zone de recherche inversée avec des enregistrements PTR pour chaque appliance de gestion VCF et hôte Amazon EVS de votre déploiement, comme indiqué dans. the section called "Création d'un environnement Amazon EVS"

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

> **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.

Configuration du serveur NTP

Les serveurs NTP fournissent le temps à votre réseau. Vous pouvez saisir les IPv4 adresses d'un maximum de quatre serveurs NTP (Network Time Protocol). Pour plus d'informations sur la configuration des serveurs NTP dans un jeu d'options DHCP, voir Création d'un jeu d'options DHCP.

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

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 le service Amazon Time Sync, consultez Définir l'heure pour votre instance dans le guide de EC2 l'utilisateur Amazon.

(Facultatif) Configurer la connectivité réseau sur site à l'aide AWS Direct Connect d' AWS Site-to-Site un VPN avec AWS Transit Gateway

Vous pouvez configurer la connectivité entre votre centre de données sur site et votre AWS infrastructure à l'aide AWS Direct Connect d'une passerelle de transit associée ou d'une AWS Site-to-Site connexion VPN à une passerelle de transit. AWS Site-to-Site Le VPN crée une connexion IPsec VPN avec la passerelle de transit via Internet. AWS Direct Connect crée une connexion IPsec VPN vers la passerelle de transit via une connexion dédiée privée. Une fois l'environnement Amazon EVS créé, vous pouvez utiliser l'une ou l'autre option pour connecter les pare-feux de votre centre de données sur site à l' VMware environnement NSX.

> **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.

Pour plus d'informations sur la configuration d'une AWS Direct Connect connexion, consultez la section Passerelles et associations de AWS 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.

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 homologue configuré sur les homologues du serveur de route doit correspondre, et les adresses IP des homologues doivent être uniques.

> **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.

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

> **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, consultez la section 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.

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**
>
> 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.

> **Note**
>
> Les opérations Amazon EVS déclenchées depuis la console Amazon EVS ne CloudTrail généreront pas d'événements.

2. Dans le panneau de navigation, choisissez Environments (Environnements).
3. Choisissez Create environment.
4. Sur la page de validation des exigences d'Amazon EVS, procédez comme suit.
   a. Vérifiez que les exigences de AWS Support et de quota de service sont respectées. Pour plus d'informations sur les exigences de support d'Amazon EVS, consultezthe section called “Souscrivez à un AWS plan Business, AWS Enterprise On-Ramp ou AWS Enterprise Support”. Pour plus d'informations sur les exigences en matière de quotas Amazon EVS, consultezthe section called “Quotas de service”.
   b. (Facultatif) Dans Nom, entrez un nom d'environnement.
   c. Pour la version Environment, choisissez votre version VCF. Amazon EVS ne prend actuellement en charge que la version 5.2.1.x.
   d. Dans le champ Site ID, entrez votre ID de site Broadcom.
   e. Pour la clé de solution VCF, entrez une clé de solution 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**
>
> 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.

f. 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**
>
> Amazon EVS exige que vous conserviez une clé de licence vSAN valide dans SDDC Manager pour que le service fonctionne 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.

g. 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.

h. Choisissez Suivant.

5. Sur la page Spécifier les détails de l'hôte, effectuez les étapes suivantes 4 fois pour ajouter 4 hôtes à l'environnement. Les environnements Amazon EVS nécessitent 4 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.

> **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.

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

e. Choisissez Ajouter un hôte.

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

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

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

c. Pour le groupe de sécurité (facultatif), vous pouvez choisir jusqu'à 2 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.

d. Sous Connectivité de gestion, entrez les blocs CIDR à utiliser pour les sous-réseaux Amazon EVS VLAN.

> **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 à la mise en réseau Amazon EVS”.

e. 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.

> **Note**
>
> Assurez-vous que les blocs d'adresse CIDR du VLAN que vous fournissez sont correctement dimensionnés dans le VPC. Pour de plus amples informations, veuillez consulter the section called "Considérations relatives à la mise en réseau Amazon EVS".

f. Sous Connectivité workload/VCF, entrez le bloc CIDR pour le VLAN de liaison montante NSX et choisissez 2 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 2 points de terminaison de serveur de route et à 2 homologues de serveur de route. 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".

g. 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.

> **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 plus d'informations sur les exigences de support d'Amazon EVS, consultezthe section called "Souscrivez à un AWS plan Business, AWS Enterprise On-Ramp ou AWS Enterprise Support". Pour plus d'informations sur les exigences en matière de quotas Amazon EVS, consultezthe section called "Quotas de service".

> **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.

- 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 le moment`--vcf-version`, Amazon EVS ne prend en charge que VCF 5.2.1.x.
- 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 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.

> **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 à la mise en 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.

  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 2 points de terminaison de serveur de route et à 2 homologues de serveur de route. 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 identifiant permet d'accéder au portail Broadcom et vous est fourni par Broadcom à la fin de votre contrat logiciel ou au renouvellement de votre contrat.

- (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-5.2.1 \
--terms-accepted \
--license-info "{
      \"solutionKey\": \"00000-00000-00000-abcde-11111\",
      \"vsanKey\": \"00000-00000-00000-abcde-22222\"
    }" \
   --initial-vlans "{
      \"vmkManagement\": {
        \"cidr\": \"10.10.0.0/24\"
      },
      \"vmManagement\": {
        \"cidr\": \"10.10.1.0/24\"
      },
      \"vMotion\": {
        \"cidr\": \"10.10.2.0/24\"
      },
      \"vSan\": {
        \"cidr\": \"10.10.3.0/24\"
      },
      \"vTep\": {
        \"cidr\": \"10.10.4.0/24\"
      },
      \"edgeVTep\": {
        \"cidr\": \"10.10.5.0/24\"
      },
      \"nsxUplink\": {
        \"cidr\": \"10.10.6.0/24\"
      },
      \"hcx\": {
        \"cidr\": \"10.10.7.0/24\"
      },
      \"expansionVlan1\": {
        \"cidr\": \"10.10.8.0/24\"
      },
      \"expansionVlan2\": {
          \"cidr\": \"10.10.9.0/24\"
```

```
      }
    }" \
--hosts "[
    {
      \"hostName\": \"esx01\",
      \"keyName\": \"sshKey-04-05-45\”,
      \"instanceType\": \"i4i.metal\"
    },
    {
      \"hostName\": \"esx02\",
      \"keyName\": \"sshKey-04-05-45\",
      \"instanceType\": \"i4i.metal\"
    },
    {
      \"hostName\": \"esx03\",
      \"keyName\": \"sshKey-04-05-45\",
      \"instanceType\": \"i4i.metal\"
    },
    {
      \"hostName\": \"esx04\",
      \"keyName\": \"sshKey-04-05-45\",
      \"instanceType\": \"i4i.metal\"
    }
  ]" \
--connectivity-info "{
    \"privateRouteServerPeerings\": [\"rsp-1234567890abcdef0\",\"rsp-
abcdef01234567890\"]
  }" \
  --vcf-hostnames "{
    \"vCenter\": \"vcf-vc01\",
    \"nsx\": \"vcf-nsx\",
    \"nsxManager1\": \"vcf-nsxm01\",
    \"nsxManager2\": \"vcf-nsxm02\",
    \"nsxManager3\": \"vcf-nsxm03\",
    \"nsxEdge1\": \"vcf-edge01\",
    \"nsxEdge2\": \"vcf-edge02\",
    \"sddcManager\": \"vcf-sddcm01\",
    \"cloudBuilder\": \"vcf-cb01\"
  }" \
--site-id my-site-id \
--region us-east-2
```

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

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'`environmentStateestCREATED`.

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

Associer des sous-réseaux VLAN Amazon EVS à une table de routage

Associez 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.

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
```

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 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.

> **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.

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 à des dispositifs de gestion VCF tels que vCenter Server, NSX et SDDC Manager. Pour plus d'informations sur la récupération de secrets, voir Obtenir des secrets depuis le Gestionnaire de AWS secrets.

> **Note**
>
> Amazon EVS ne propose pas de rotation gérée de vos secrets. Nous vous recommandons de faire régulièrement alterner vos secrets selon une fenêtre de rotation définie afin de vous assurer qu'ils ne durent pas 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

Par défaut, Amazon EVS active le ESXi 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 ESXi hôte localement.

> **Note**
>
> Amazon EVS désactive le SSH à distance par défaut. Pour plus d'informations sur l'activation de SSH pour accéder au ESXi shell distant, consultez la section Remote ESXi 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

SDDC UI and Amazon EVS console

1. Accédez à l'interface utilisateur de SDDC Manager.

2. Supprimez les hôtes du cluster vSphere. Cela annulera l'attribution des hôtes au domaine SDDC. Répétez cette étape pour chaque hôte du cluster. Pour plus d'informations, consultez Supprimer un hôte d'un cluster vSphere dans un domaine de charge de travail dans la documentation du produit VCF.
3. Mettez hors service les hôtes non assignés. Pour plus d'informations, consultez la section Démission des hôtes dans la documentation du produit VCF.
4. Accédez à la console Amazon EVS.

> **Note**
>
> Les opérations Amazon EVS déclenchées depuis la console Amazon EVS ne CloudTrail généreront pas d'événements.

5. Dans le volet de navigation, choisissez Environment.
6. Sélectionnez l'environnement qui contient les hôtes à supprimer.
7. Sélectionnez l'onglet Hosts.
8. Sélectionnez l'hôte et choisissez Supprimer dans l'onglet Hôtes. Répétez cette étape pour chaque hôte de l'environnement.
9. 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.

10. 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.

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

3. Accédez à l'interface utilisateur de SDDC Manager.
4. Supprimez les hôtes du cluster vSphere. Cela annulera l'attribution des hôtes au domaine SDDC. Répétez cette étape pour chaque hôte du cluster. Pour plus d'informations, consultez Supprimer un hôte d'un cluster vSphere dans un domaine de charge de travail dans la documentation du produit VCF.
5. Mettez hors service les hôtes non assignés. Pour plus d'informations, consultez la section Démission des hôtes dans la documentation du produit VCF.
6. 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
```

7. Répétez les étapes précédentes pour supprimer les hôtes restants de votre environnement.
8. 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.

9. 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 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.

Supprimer les interfaces réseau élastiques

Pour savoir comment supprimer des interfaces réseau élastiques, consultez la section Supprimer une interface réseau dans le guide de EC2 l'utilisateur Amazon.

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.

Supprimer 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.

Supprimer le 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.

Migrez les charges de travail vers Amazon EVS à l'aide de l'extension de cloud VMware hybride (HCX) VMware

> **Note**
>
> Amazon EVS est en version préliminaire publique et est sujet à modification.

Après avoir créé un environnement Amazon EVS, vous pouvez migrer vos charges de travail existantes VMware vers Amazon Elastic VMware Service (Amazon EVS) à l'aide de l'extension VMware Hybrid Cloud (VMware HCX). Pour plus d'informations sur la migration VMware HCX, consultez la section Types de migration VMware HCX dans le guide de l'utilisateur VMware HCX.

Le didacticiel suivant explique comment utiliser VMware HCX pour migrer une VMware charge de travail vers Amazon EVS.

Vous pouvez utiliser VMware HCX pour migrer des charges de travail via une connexion privée à l'aide AWS Direct Connect d'une passerelle de transit associée ou à l'aide d'un rattachement AWS Site-to-Site VPN à une passerelle de transit.

> **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.

Pour plus d'informations sur la configuration d'une AWS Direct Connect connexion, consultez la section Passerelles et associations de AWS Direct Connect passerelles de transit dans le Guide de l' AWS Direct Connect utilisateur. 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.

Prérequis

Avant d'utiliser VMware HCX avec Amazon EVS, assurez-vous que les prérequis HCX sont remplis et qu'un environnement Amazon EVS a été créé et connecté à votre réseau sur site à l'aide d'une

passerelle de transit ou AWS Site-to-Site d'un VPN AWS Direct Connect avec une passerelle de transit. Pour connaître les étapes de création d'un environnement Amazon EVS, consultezPremiers pas. Pour plus d'informations sur les prérequis VMware HCX, consultez. the section called "VMware Prérequis HCX"

Vérifiez l'état du sous-réseau VLAN HCX

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.
6. Copiez l'`vlan`identifiant HCX pour une utilisation ultérieure.

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
```

Voici un exemple de réponse.

```
{
 "environmentVlans": [
        {
            "vlan": 80,
            "cidr": "10.10.7.0/24",
            "availabilityZone": "us-east-2c",
            "functionName": "hcx",
            "createdAt": "2025-04-13T13:39:58.845000+00:00",
```

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


2. Identifiez le VLAN avec un `functionName` de `hcx` et vérifiez que c'`vlanState`est `CREATED` le cas.
3. Copiez l'`vlan`identifiant HCX pour une utilisation ultérieure.

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”.

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.

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

Le service d'optimisation WAN HCX (HCX-WAN-OPT) 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-WAN-IX). HCX-WAN-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, en évitant 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.

Sécurité dans Amazon Elastic VMware Service

> **Note**
>
> Amazon EVS est en version préliminaire publique et est sujet à modification.

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, 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 la sensibilité de vos données, les exigences de votre entreprise et la législation et la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation d'Amazon Elastic VMware Service. Il vous explique comment configurer Amazon Elastic VMware Service 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 Elastic VMware Service.

Table des matières

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

Gestion des identités et des accès pour Amazon Elastic VMware Service

> **Note**
>
> Amazon EVS est en version préliminaire publique et est sujet à modification.

AWS Identity and Access Management (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. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- Public ciblé
- Authentification par des identités
- Gestion des accès à l'aide de politiques
- Comment fonctionne Amazon Elastic VMware Service avec IAM
- Exemples de politiques basées sur l'identité Amazon EVS
- Résolution des problèmes d'identité et d'accès à Amazon Elastic VMware Service
- AWS politiques gérées pour Amazon EVS
- Utilisation de rôles liés à un service pour Amazon EVS

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans Amazon Elastic VMware Service.

Utilisateur du service : si vous utilisez le service Amazon Elastic VMware Service 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 VMware de fonctionnalités d'Amazon Elastic Service dans le cadre de votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur.

Administrateur du service : si vous êtes responsable des ressources Amazon Elastic VMware Service au sein de votre entreprise, vous avez probablement un accès complet à Amazon Elastic VMware Service. C'est à vous de déterminer les fonctionnalités et les ressources d'Amazon Elastic VMware Service 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 Elastic VMware Service, consultezthe section called "Comment fonctionne Amazon Elastic VMware Service 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 Elastic VMware Service. Pour consulter des exemples de politiques basées sur l'identité Amazon Elastic VMware Service que vous pouvez utiliser IAM, consultez les exemples de politiques basées sur l'identité Amazon Elastic VMware Service.

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 compte AWS 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 d'AWS Sign-In.

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 les références générales d'AWS.

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 le guide de l'utilisateur d'AWS IAM Identity Center (successeur d'AWS Single Sign-On) et l'utilisation de l'authentification multifactorielle (MFA AWS) dans le guide de l'utilisateur IAM.

Utilisateur racine d'un compte AWS

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 racine du compte AWS et elle est accessible après connexion à l'aide de l'adresse e-mail et du mot de passe utilisés pour la création du compte. Il est vivement recommandé de ne pas utiliser l'utilisateur root pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur root 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 d'AWS Single Sign-On).

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 le guide de l'utilisateur d'AWS IAM Identity Center (successeur d'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 d'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 à un service apparaissent dans votre Compte AWS répertoire 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 des 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 leurs propres mots 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. La SCP limite les autorisations pour les entités dans les comptes membres, y compris dans chaque utilisateur racine d'un compte AWS. Pour plus d'informations sur les organisations SCPs, consultez la section Comment SCPs travailler dans le guide de l'utilisateur d'AWS Organizations.
- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance 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 Elastic VMware Service avec IAM

> **Note**
>
> Amazon EVS est en version préliminaire publique et est sujet à modification.

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

IAM fonctionnalité	Assistance Amazon EVS
the section called “Politiques basées sur l'identité pour Amazon EVS”	Oui
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

IAM fonctionnalité	Assistance Amazon EVS
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 Elastic VMware Service et les autres Services AWS services fonctionnent IAM, consultez Services AWS le guide IAM de l'utilisateur d'IAM.

Rubriques

- Politiques basées sur l'identité pour Amazon EVS
- Listes de contrôle d'accès (ACLs) dans Amazon EVS
- Contrôle d'accès basé sur les attributs (ABAC) avec Amazon EVS
- Utilisation d'informations d'identification temporaires avec Amazon EVS
- Transférer les sessions d'accès pour Amazon EVS
- Rôles de service pour Amazon EVS
- Rôles liés à un service pour Amazon EVS

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 d'Amazon Elastic VMware Service, consultez les exemples de politiques basées sur l'identité d'Amazon Elastic VMware Service.

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 stratégies 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 Elastic VMware Service 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 Elastic VMware Service 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 Elastic VMware Service, consultez la section Actions définies par Amazon Elastic VMware Service dans la référence d'autorisation du service.

Ressources relatives aux politiques pour Amazon EVS

Supporte les ressources politiques : partielles

Les administrateurs peuvent utiliser les stratégies 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 l'instruction 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 stratégies 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 Elastic VMware Service 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 Elastic VMware Service, consultez la section Clés de condition pour Amazon Elastic VMware Service dans la référence d'autorisation du service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez Actions définies par Amazon Elastic VMware Service.

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 Elastic VMware Service ou transmettre des balises dans une demande adressée à Amazon Elastic VMware Service. 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 Transmission 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 aux services : 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 Elastic VMware Service, consultez. the section called “Utilisation des rôles liés à un service”

Exemples de politiques basées sur l'identité Amazon EVS

> **Note**
>
> Amazon EVS est en version préliminaire publique et est sujet à modification.

Par défaut, Utilisateurs IAM les rôles ne sont pas autorisés à créer ou à modifier les ressources Amazon Elastic VMware Service. 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
- Utilisation de la console Amazon Elastic VMware Service
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations
- Création et gestion d'un environnement Amazon EVS
- Obtenez et listez les environnements Amazon EVS, les hôtes et VLANs

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer des ressources Amazon Elastic VMware Service 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 AWS 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 la 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 Elastic VMware Service

Pour accéder à la console Amazon Elastic VMware Service, un responsable 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 Elastic VMware Service présentes

dans votre Compte AWS. 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 attachée.

Pour vous assurer que vos responsables IAM peuvent toujours utiliser la console Amazon Elastic VMware Service, 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. N'autorisez plutôt l'accès qu'aux actions correspondant à l'opération d'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"
            ],
            "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 Elastic VMware Service

> **Note**
>
> Amazon EVS est en version préliminaire publique et est sujet à modification.

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lors de l'utilisation d'Amazon Elastic VMware Service et IAM.

Rubriques

- AccessDeniedException
- Je souhaite autoriser des personnes extérieures Compte AWS à moi à accéder à mes ressources Amazon Elastic VMware Service

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 Compte AWS à moi à accéder à mes ressources Amazon Elastic VMware Service

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 Elastic VMware Service prend en charge ces fonctionnalités, consultezthe section called "Comment fonctionne Amazon Elastic VMware Service 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

> **Note**
>
> Amazon EVS est en version préliminaire publique et est sujet à modification.

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 politique 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 vous 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 permet au rôle lié au service d'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`- Créez, modifiez, balisez et supprimez une interface réseau élastique utilisée pour établir une connexion permanente entre Amazon EVS et une appliance SDDC Manager de VMware Virtual Cloud Foundation (VCF) dans le sous-réseau VPC du client. Cette connectivité est requise pour qu'Amazon EVS puisse déployer, gérer et surveiller le déploiement du VCF.

Pour consulter 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.

Modification	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

> **Note**
>
> Amazon EVS est en version préliminaire publique et est sujet à modification.

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 d'approbation 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 Yes (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` Le rôle permet à Amazon EVS de gérer les clusters de votre compte. Les politiques jointes permettent au rôle de gérer les ressources suivantes : interfaces réseau, groupes de sécurité, journaux et VPCs.

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

Il n'est pas nécessaire de créer manuellement un rôle lié à un service. Lorsque vous créez un cluster 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. Une fois que vous avez 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 IAM Guide de l'utilisateur.

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.

Nettoyer 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 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 de plus amples informations, veuillez consulter Points de terminaison et quotas.

Utilisation d'Amazon EVS avec d'autres services AWS

> **Note**
>
> Amazon EVS est en version préliminaire publique et est sujet à modification.

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
- Exécutez des charges de travail à hautes performances avec Amazon FSx pour ONTAP NetApp

Créez des ressources Amazon EVS avec AWS CloudFormation

> **Note**
>
> Amazon EVS est en version préliminaire publique et est sujet à modification.

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

> **Note**
>
> Amazon EVS est en version préliminaire publique et est sujet à modification.

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 banque de données NFS/iSCSI et en tant que stockage connecté aux clients pour les machines virtuelles exécutées sur Amazon EVS. VMware

Configuration FSx pour NetApp ONTAP en tant que banque de données NFS

> **Note**
>
> Amazon EVS est en version préliminaire publique et est sujet à modification.

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.

Prérequis

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 Premiers pas.
- 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.

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 for Single-AZ 1 or at least 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 aux services".
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. Vérifiez 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

> **Note**
>
> Amazon EVS est en version préliminaire publique et est sujet à modification.

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.

Prérequis

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 Premiers pas.
- 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.

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 for Single-AZ 1 or at least 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 aux services".
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. Passez en revue les attributs du système de fichiers et choisissez Créer un système de fichiers.

Configuration d'un adaptateur iSCSI logiciel dans vSphere pour le stockage hôte ESXi

Pour chaque ESXi hôte, vous devez configurer l'adaptateur iSCSI logiciel afin que vos ESXi hôtes puissent l'utiliser pour accéder au stockage iSCSI. Pour obtenir des instructions sur la configuration de l'adaptateur logiciel iSCSI pour les ESXi hôtes de 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'unités logiques (LUNs) spécifiquement destinés à l'accès iSCSI, fournissant ainsi un stockage par blocs partagé à ESXi vos hôtes. 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 ESXi hôtes 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 ESXi hôte dans la documentation du produit VMware vSphere.

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

> **Note**
>
> Amazon EVS est en version préliminaire publique et est sujet à modification.

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 sur votre environnement afin d'identifier les problèmes. Vous pouvez consulter l'état de votre environnement pour identifier les 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 atteindre l'environnement, cette vérification échoue.

Si cette vérification échoue, Amazon EVS ne peut plus contacter SDDC Manager pour valider l'état de l'environnement, et les hôtes ne peuvent plus être ajoutés à l'environnement. Une défaillance de

l'accessibilité entraînera également l'échec de la réutilisation des clés de licence et des vérifications de couverture des clés, et la vérification du nombre d'hôtes entraînera le renvoi d'une réponse inconnue.

Les défaillances d'accessibilité indiquent qu'il peut y avoir un problème avec le gestionnaire SDDC, la configuration du pare-feu ou un certificat manquant. Vous pouvez essayer de résoudre ces problèmes ou 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 5.2.1.

Si cette vérification échoue, vous devrez ajouter des hôtes afin que votre environnement réponde à cette exigence minimale. Amazon EVS prend uniquement en charge les environnements de 4 à 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 pour un seul environnement Amazon EVS. Cette vérification échoue si une licence d'occasion est ajoutée à l'environnement.

Si cette vérification échoue, vous recevez une réponse d'erreur indiquant que l'environnement Amazon EVS n'a pas pu être créé. Pour résoudre le problème, passez en revue vos paramètres de licence dans SDDC Manager et remplacez les licences précédemment utilisées par des licences non utilisées.

> **Important**
>
> Utilisez l'interface utilisateur de SDDC Manager pour gérer les clés de licence des composants VCF. Amazon EVS exige que vous conserviez des clés de licence de composant valides dans SDDC Manager pour que le service fonctionne correctement. Si vous gérez les clés de licence des composants 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 afin d'éviter tout échec de la vérification des clés de licence.

La vérification de la couverture des clés a échoué

Cette vérification permet de vérifier que la clé de licence VCF attribuée à vCenter Server alloue suffisamment de cœurs de vCPU et de capacité de stockage vSAN (TiB) pour tous les hôtes déployés.

Si cette vérification échoue, vous recevez une réponse d'erreur indiquant que l'environnement Amazon EVS n'a pas pu être créé ou qu'aucun hôte Amazon EVS n'a pu être ajouté à l'environnement. Une défaillance de couverture clé peut indiquer l'un des problèmes suivants :

- Vous avez dépassé le nombre d'hôtes pris en charge pour Amazon EVS. Amazon EVS prend en charge 4 à 16 hôtes par environnement. Si tel est le cas, supprimez ou ajoutez des hôtes jusqu'à ce que votre environnement soit dans la plage d'hôtes prise en charge.
- 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 avant l'expiration de la licence actuellement attribuée. Si tel est le cas, passez en revue les attributions de licence 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 une capacité vSAN d'au moins 110 TiB. Si tel est le problème, ajoutez des licences vSAN dans SDDC Manager jusqu'à ce que vos besoins 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 de SDDC Manager pour gérer les clés de licence des composants VCF. Amazon EVS exige que vous conserviez des clés de licence de composant valides dans SDDC Manager pour que le service fonctionne correctement. Si vous gérez les clés de licence des composants 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 afin d'éviter tout échec de la vérification des clés de licence.

L'agent vSphere HA sur cet hôte n'a pas pu atteindre l'adresse d'isolement

Dans l'interface utilisateur de vCenter, lorsque l' ESXi hôte 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.

Pour supprimer le message d'erreur vSphere HA, vous devez désactiver vSphere HA. Pour savoir comment désactiver vSphere HA dans le client vSphere, consultez l'article de Broadcom sur la désactivation et l'activation de la haute disponibilité (HA). VMware

Points de terminaison et quotas Amazon Elastic VMware Service

> **Note**
>
> Amazon EVS est en version préliminaire publique et est sujet à modification.

Vous trouverez ci-dessous les points de terminaison et les quotas de service pour ce service. Pour vous connecter par programmation à un Service AWS, vous utilisez un point de terminaison. Outre les points de AWS terminaison standard, certains Services AWS proposent des points de terminaison FIPS dans certaines régions. Pour plus d'informations, consultez Points de terminaison du service AWS. Les quotas de service, également appelés limites, représentent le nombre maximal de ressources ou d'opérations de service pour votre Compte AWS. Pour plus d'informations, consultez Quotas de service AWS.

Points de terminaison de service

L'API Amazon EVS fournit des points de terminaison régionaux et à double pile, ainsi que des points de terminaison FIPS pour les régions des États-Unis. Pour utiliser les points de terminaison à double pile avec le AWS CLI, consultez la configuration des points de terminaison à double pile et FIPS dans le AWS SDKs guide de référence des outils et.

Nom de la région	Région	Point de terminaison	Protocole
USA Est (Virginie du Nord)	us-east-1	evs.us-east-1.amazonaws.com evs-fips.us-east-1.amazonaws.com evs.us-east-1.api.aws evs-fips.us-east-1.api.aws	HTTPS
USA Est (Ohio)	us-east-2	evs.us-east-2.amazonaws.com evs-fips.us-east-2.amazonaws.com	HTTPS

Nom de la région	Région	Point de terminaison	Protocole
		evs.us-east-2.api.aws evs-fips.us-east-2.api.aws	
USA Ouest (Oregon)	us-west-2	evs.us-west-2.amazonaws.com evs-fips.us-west-2.amazonaws.com evs.us-west-2.api.aws evs-fips.us-west-2.api.aws	HTTPS
Asie-Pacifique (Tokyo)	ap-northeast-1	evs.ap-northeast-1.amazonaws.com evs.ap-northeast-1.api.aws	HTTPS
Europe (Francfort)	eu-central-1	evs.eu-central-1.amazonaws.com evs.eu-central-1.api.aws	HTTPS
Europe (Irlande)	eu-west-1	evs.eu-west-1.amazonaws.com evs.eu-west-1.api.aws	HTTPS

Quotas de service

Important

Pour permettre la création d'un environnement Amazon EVS, votre nombre d'hôtes par quota d'environnement EVS doit être d'au moins 4. Le quota par défaut est 0. Pour augmenter ce quota, accédez à la console Service Quotas et demandez une augmentation de quota.

Note

Si vous prévoyez d'utiliser des hôtes EC2 dédiés pour votre environnement Amazon EVS, assurez-vous que la valeur de votre quota d'hôtes EC2 dédiés reflète le nombre d'hôtes dédiés que vous avez l'intention d'utiliser pour la région souhaitée. Les déploiements VCF

nécessitent un minimum de 4 hôtes. Pour plus d'informations, consultez Amazon EC2 Dedicated Hosts.

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.

Nom	Par défaut	Ajustable	Description
Nombre d'hôtes par environnement EVS	0	Oui	Nombre maximum d'hôtes pouvant être provisionnés dans un seul environnement Amazon EVS.

Historique du document pour le guide de l'utilisateur d'Amazon Elastic VMware Service

> **Note**
>
> Amazon EVS est en version préliminaire publique et est sujet à modification.

Le tableau suivant décrit les versions de documentation pour Amazon Elastic VMware Service.

Modification	Description	Date
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. 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.