Sécurité vSphere

ESXi 6.5
vCenter Server 6.5

Ce document prend en charge la version de chacun des produits répertoriés, ainsi que toutes les versions publiées par la suite jusqu'au remplacement dudit document par une nouvelle édition. Pour rechercher des éditions plus récentes de ce document, rendez-vous sur : http://www.vmware.com/fr/support/pubs.

FR-002011-00

vmware®

Vous trouverez la documentation technique la plus récente sur le site Web de VMware à l'adresse :

http://www.vmware.com/fr/support/

Le site Web de VMware propose également les dernières mises à jour des produits.

N'hésitez pas à nous transmettre tous vos commentaires concernant cette documentation à l'adresse suivante :

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware, Inc.
100-101 Quartier Boieldieu
92042 Paris La Défense
France
www.vmware.com/fr

Table des matières

À propos de la sécurité de vSphere

Sécurité vSphere fournit des informations sur la sécurisation de votre environnement vSphere® pour VMware® vCenter® Server et VMware ESXi.

Pour vous aider à protéger votre environnement vSphere, cette documentation décrit les fonctionnalités de sécurité disponibles et les mesures à prendre pour protéger votre environnement des attaques.

Documentation connexe

Un document de complément, *Administration de Platform Services Controller* , explique comment utiliser les services de Platform Services Controller, par exemple pour gérer l'authentification avec vCenter Single Sign-On et pour gérer les certificats dans l'environnement vSphere.

Outre ces documents, VMware publie un *Guide de sécurisation renforcée* pour chaque version de vSphere. Ces guides sont disponibles à la page http://www.vmware.com/security/hardening-guides.html. Le *Guide de sécurisation renforcée* est une feuille de calcul comprenant des entrées pour différents problèmes potentiels de sécurité. Il offre des éléments pour trois profils de risque. Ce document *Sécurité vSphere* ne contient pas d'informations concernant le profil de risque 1 (environnement imposant une sécurité maximale, comme les installations gouvernementales top secrètes).

Public cible

Ces informations sont destinées aux administrateurs système Windows ou Linux expérimentés qui maîtrisent les technologies de machine virtuelle et les opérations de centre de données.

vSphere Web Client et vSphere Client (Client HTML 5)

Les instructions relatives aux tâches présentées dans ce guide se basent sur vSphere Web Client. Vous pouvez également exécuter la plupart des tâches de ce guide en utilisant la nouvelle version de vSphere Client. La terminologie, la topologie et le workflow de la nouvelle interface utilisateur de vSphere Client correspondent fidèlement aux aspects et éléments de l'interface utilisateur de vSphere Web Client. Vous pouvez appliquer les instructions de vSphere Web Client à la nouvelle version de vSphere Client sauf mention du contraire.

Remarque Les fonctionnalités de vSphere Web Client n'ont pas toutes été mises en œuvre pour vSphere Client dans la version vSphere 6.5. Pour obtenir une liste actualisée des fonctionnalités non prises en charge, consultez le *Guide des mises à jour des fonctionnalités de vSphere Client* sur http://www.vmware.com/info?id=1413.

Sécurité dans l'environnement vSphere 1

Les composants d'un environnement vSphere sont sécurisés d'origine par plusieurs fonctionnalités telles que l'authentification, l'autorisation, un pare-feu sur chaque hôte ESXi, etc. Vous pouvez modifier la configuration par défaut de plusieurs manières. Vous pouvez notamment définir des autorisations sur des objets vCenter, ouvrir des ports de pare-feu ou modifier les certificats par défaut. Vous pouvez prendre des mesures de sécurité sur différents objets dans la hiérarchie d'objets vCenter, comme les systèmes vCenter Server, les hôtes ESXi, les machines virtuelles et les objets du réseau et de stockage.

Une présentation globale des différentes parties de vSphere à surveiller vous aide à planifier votre stratégie de sécurité. Vous pouvez également tirer parti d'autres ressources de sécurité de vSphere sur le site Web VMware.

Ce chapitre aborde les rubriques suivantes :

Sécurisation de l'hyperviseur ESXi

L'hyperviseur ESXi est sécurisé par nature. Vous pouvez renforcer la protection des hôtes ESXi en utilisant le mode de verrouillage et d'autres fonctionnalités intégrées. À des fins d'uniformité, vous pouvez définir un hôte de référence et laisser tous les hôtes en synchronisation avec le profil de l'hôte de référence. Vous pouvez également protéger votre environnement en effectuant une gestion chiffrée, qui garantit que les modifications sont appliquées à tous les hôtes.

Utilisez les fonctionnalités suivantes (présentées en détail dans ce guide) pour renforcer la protection des hôtes ESXi gérés par vCenter Server. Reportez-vous également au livre blanc *Sécurité de VMware vSphere Hypervisor*.

Limiter l'accès à ESXi Par défaut, les services ESXi Shell et SSH ne s'exécutent pas et seul l'utilisateur racine peut se connecter à l'interface utilisateur de la console directe (DCUI). Si vous décidez d'activer l'accès à ESXi ou SSH, vous pouvez définir des délais d'expiration pour limiter le risque d'accès non autorisé.

Les hôtes pouvant accéder à l'hôte ESXi doivent disposer d'autorisations de gestion de l'hôte. Ces autorisations se définissent sur l'objet hôte du système vCenter Server qui gère l'hôte.

Utiliser des utilisateurs nommés et le moindre privilège

Par défaut, l'utilisateur racine peut effectuer de nombreuses tâches. Au lieu d'autoriser les administrateurs à se connecter à l'hôte ESXi à l'aide du compte d'utilisateur racine, vous pouvez appliquer des privilèges de configuration de l'hôte différents à divers utilisateurs nommés à partir de l'interface de gestion des autorisations de vCenter Server. Vous pouvez créer un rôle personnalisé, attribuer des privilèges à un rôle et associer le rôle à un utilisateur nommé ou un groupe d'utilisateurs nommés et à un objet hôte d'ESXi en utilisant vSphere Web Client.

Si vous gérez les utilisateurs directement sur l'hôte, les options de gestion des rôles sont limitées. Consultez la documentation de *Gestion individuelle des hôtes vSphere - VMware Host Client*.

Réduire le nombre de ports de pare-feu ESXi ouverts

Par défaut, les ports de pare-feu de votre hôte ESXi sont uniquement ouverts lorsque vous démarrez un service correspondant. Vous pouvez utiliser les commandes de vSphere Web Client, ESXCLI ou PowerCLI pour vérifier et gérer l'état des ports du pare-feu.

Reportez-vous à « ESXi », page 67.

Automatiser la gestion des hôtes ESXi

Parce qu'il est souvent important que les différents hôtes d'un même centre de données soient synchronisés, utilisez l'installation basée sur scripts ou vSphere Auto Deploy pour provisionner les hôtes. Vous pouvez gérer les hôtes à l'aide de scripts. Les profils d'hôte sont une alternative à la gestion chiffrée. Vous définissez un hôte de référence, exportez le profil d'hôte et appliquez celui-ci à tous les hôtes. Vous pouvez appliquer le profil d'hôte directement ou dans le cadre du provisionnement avec Auto Deploy.

Consultez « Utiliser des scripts pour gérer des paramètres de configuration d'hôte », page 43 et *Installation et configuration de vSphere* pour plus d'informations sur vSphere Auto Deploy.

Exploiter le mode de verrouillage

En mode de verrouillage, les hôtes ESXi sont, par défaut, uniquement accessibles par le biais de vCenter Server. À partir de vSphere 6.0, vous avez le choix entre un mode de verrouillage strict et un mode de verrouillage normal. Vous pouvez également définir des utilisateurs exceptionnels pour permettre un accès direct aux comptes de service tels que les agents de sauvegarde.

Reportez-vous à « Mode verrouillage », page 76.

Vérifier l'intégrité du module VIB

Un niveau d'acceptation est associé à chaque module VIB. Vous pouvez ajouter un VIB à un hôte ESXi uniquement si son niveau d'acceptation est identique ou supérieur au niveau d'acceptation de l'hôte. Vous ne pouvez pas ajouter un VIB CommunitySupported ou PartnerSupported à un hôte à moins d'avoir explicitement modifié le niveau d'acceptation de l'hôte.

Reportez-vous à « Vérifier les niveaux d'acceptation des hôtes et des fichiers VIB », page 83.

Gérer les certificats ESXi

Dans vSphere 6.0 et version ultérieure, VMware Certificate Authority (VMCA) provisionne chaque hôte ESXi à l'aide d'un certificat signé dont l'autorité de certification racine par défaut est VMCA. Si la stratégie de l'entreprise l'exige, vous pouvez remplacer les certificats existants par des certificats signés par une autorité de certification d'entreprise ou tierce.

Reportez-vous à « Gestion de certificats pour les hôtes ESXi », page 52

Authentification par carte à puce

À partir de vSphere 6.0, ESXi prend en charge l'option d'authentification par carte à puce plutôt que par nom d'utilisateur et mot de passe.

Reportez-vous à « Configuration de l'authentification par carte à puce pour ESXi », page 94.

Verrouillage de compte ESXi

À partir de vSphere 6.0, le verrouillage des comptes est pris en charge pour l'accès via SSH et vSphere Web Services SDK. Par défaut, un nombre maximal de dix tentatives de connexion échouées est autorisé avant le verrouillage du compte. Par défaut, le compte est déverrouillé au bout de deux minutes. L'interface de console directe (DCUI) et ESXi Shell ne prennent pas en charge le verrouillage de compte.

Reportez-vous à « Verrouillage des mots de passe et des comptes ESXi », page 45.

Les considérations de sécurité pour les hôtes autonomes sont identiques, bien que les tâches de gestion puissent différer. Reportez-vous à la documentation et *Gestion individuelle des hôtes vSphere - VMware Host Client*.

Sécurisation des systèmes vCenter Server et services associés

Votre système vCenter Server et les services associés sont protégés par l'authentification via vCenter Single Sign-On, ainsi que par l'autorisation via le modèle d'autorisations vCenter Server. Vous pouvez modifier le comportement par défaut et prendre des mesures supplémentaires pour limiter l'accès à votre environnement.

Lorsque vous protégez votre environnement vSphere, tenez compte du fait que tous les services associés aux instances de vCenter Server doivent être protégés. Dans certains environnements, vous pouvez protéger plusieurs instances de vCenter Server et une ou plusieurs instances de Platform Services Controller.

Renforcer toutes les machines hôtes vCenter

Pour protéger votre environnement vCenter, vous devez commencer par renforcer chaque machine qui exécute vCenter Server ou un service associé. Ceci s'applique aussi bien à une machine physique qu'à une machine virtuelle. Installez toujours les derniers correctifs de sécurité pour votre système d'exploitation et mettez en œuvre les meilleures pratiques standard de l'industrie pour protéger la machine hôte.

En savoir plus sur le modèle de certificat vCenter

Par défaut, l'autorité de certification VMware provisionne chaque hôte ESXi, chaque machine de l'environnement et chaque utilisateur de solution à l'aide d'un certificat signé par VMCA (VMware Certificate Authority). L'environnement fourni est prêt à l'emploi, mais vous pouvez modifier le comportement par défaut si la stratégie de l'entreprise l'exige. Pour plus d'informations, reportez-vous à la documentation *Administration de Platform Services Controller* .

Pour une protection supplémentaire, supprimez explicitement les certificats révoqués ou qui ont expiré, ainsi que les installations qui ont échoué.

Configurer vCenter Single Sign-On

vCenter Server et les services associés sont protégés par la structure d'authentification vCenter Single Sign-On. Lors de la première installation des logiciels, vous devez spécifier un mot de passe pour l'administrateur du domaine vCenter Single Sign-On (par défaut, administrator@vsphere.local). Seul ce domaine est disponible initialement comme source d'identité. Vous pouvez ajouter d'autres sources d'identité (Active Directory ou LDAP) et définir une source d'identité par défaut. Dorénavant, les utilisateurs qui

peuvent s'authentifier auprès d'une de ces sources d'identité ont la possibilité d'afficher des objets et d'effectuer des tâches, dans la mesure où ils y ont été autorisés. Pour plus d'informations, reportez-vous à la documentation *Administration de Platform Services Controller* .

Attribuer des rôles à des utilisateurs ou groupes nommés

Pour optimiser la journalisation, chaque autorisation octroyée pour un objet peut être associée à un utilisateur ou groupe nommé, ainsi qu'à un rôle prédéfini ou personnalisé. Le modèle d'autorisations vSphere 6.0 procure une grande flexibilité en offrant la possibilité d'autoriser les utilisateurs et les groupes de diverses façons. Reportez-vous aux sections « Présentation des autorisations dans vSphere », page 20 et « Privilèges requis pour les tâches courantes », page 37.

Limitez les privilèges d'administrateur et l'utilisation du rôle d'administrateur. Dans la mesure du possible, évitez d'utiliser l'utilisateur Administrateur anonyme.

Configurer NTP

Configurez NTP pour chaque nœud de votre environnement. L'infrastructure de certificats exige un horodatage précis et ne fonctionne correctement que si les nœuds sont synchronisés.

Reportez-vous à « Synchronisation des horloges sur le réseau vSphere », page 185.

Sécurisation des machines virtuelles

Pour sécuriser vos machines virtuelles, appliquez tous les correctifs appropriés aux systèmes d'exploitation invités et protégez votre environnement, de même que vous protégez votre machine physique. Pensez à désactiver toutes les fonctionnalités inutiles, à minimiser l'utilisation de la console de machine virtuelle et à suivre toute autre meilleure pratique.

Protéger le système d'exploitation invité

Pour protéger votre système d'exploitation invité, assurez-vous qu'il utilise les correctifs les plus récents et, le cas échéant, des applications de logiciel anti-espion et anti-programme malveillant. Reportez-vous à la documentation du fournisseur de votre système d'exploitation invité et, le cas échéant, à d'autres informations disponibles dans des manuels ou sur Internet pour ce système d'exploitation.

Désactiver les fonctionnalités inutiles

Vérifiez que toute fonctionnalité inutile est désactivée pour minimiser les points d'attaque potentiels. De nombreuses fonctionnalités peu utilisées sont désactivées par défaut. Supprimez le matériel inutile et désactivez certaines fonctionnalités, comme HFSG ou le copier-coller entre la machine virtuelle et une console distante.

Reportez-vous à « Désactiver les fonctions inutiles à l'intérieur des machines virtuelles », page 126.

Utiliser les modèles et la gestion basée sur des scripts

Les modèles de machine virtuelle vous permettent de configurer le système d'exploitation afin qu'il respecte des conditions requises spécifiques, puis de créer d'autres machines virtuelles avec les mêmes paramètres.

Pour modifier les paramètres après le déploiement initial, vous pouvez utiliser les scripts (PowerCLI, par exemple). Cette documentation explique plusieurs tâches en utilisant vSphere Web Client pour illustrer le processus. Utiliser des scripts plutôt que vSphere Web Client peut vous aider à garder votre environnement cohérent. Dans les environnements de grande envergure, vous pouvez grouper les machines virtuelles dans des dossiers pour optimiser les scripts.

Reportez-vous à « Utiliser des modèles pour déployer des machines virtuelles », page 125. Consultez *Administration d'une machine virtuelle vSphere* pour plus d'informations.

Minimiser l'utilisation de la console de machine virtuelle

La console de machine virtuelle joue pour la machine virtuelle le même rôle qu'un moniteur sur un serveur physique. Les utilisateurs qui ont accès à la console de machine virtuelle ont accès à la gestion d'alimentation des machines virtuelles et aux contrôles de la connectivité des périphériques amovibles. Cet accès peut permettre une attaque malveillante sur une machine virtuelle.

Activer le démarrage sécurisé UEFI

À partir de vSphere 6.5, vous pouvez configurer votre machine virtuelle pour qu'elle utilise le démarrage UEFI. Si le système d'exploitation prend en charge le démarrage UEFI sécurisé, vous pouvez sélectionner cette option pour vos machines virtuelles pour plus de sécurité. Reportez-vous à « Activer ou désactiver le démarrage sécurisé UEFI pour une machine virtuelle », page 121.

Sécurisation de la couche de mise en réseau virtuelle

La couche de mise en réseau virtuelle comprend des adaptateurs réseau virtuels, des commutateurs virtuels, des commutateurs virtuels distribués, des ports et des groupes de ports. ESXi utilise la couche réseau virtuelle pour les communications entre les machines virtuelles et leurs utilisateurs. En outre, ESXi utilise cette couche de mise en réseau pour communiquer avec les SAN iSCSI, le stockage NAS, etc.

vSphere offre toutes les fonctionnalités pour garantir une infrastructure de mise en réseau sécurisée. Vous pouvez sécuriser séparément chacun des éléments de l'infrastructure (commutateurs virtuels, commutateurs virtuels distribués ou adaptateurs réseau virtuels, par exemple). En outre, tenez compte des directives suivantes, détaillées dans la section Chapitre 8, « Sécurisation de la mise en réseau vSphere », page 163.

Isoler le trafic réseau

L'isolation du trafic réseau est essentielle pour un environnement ESXi sécurisé. Des réseaux différents requièrent un accès et un niveau d'isolation distincts. Un réseau de gestion isole le trafic client, le trafic de l'interface de ligne de commande ou de l'API ou le trafic des logiciels tiers du trafic normal. Assurez-vous que seuls les administrateurs système, réseau et de la sécurité peuvent accéder au réseau de gestion.

Reportez-vous à « Recommandations de sécurité pour la mise en réseau d'ESXi », page 50.

Utiliser des pare-feu pour sécuriser les éléments du réseau virtuel

Vous pouvez ouvrir et fermer les ports de pare-feu et sécuriser les différents éléments du réseau virtuel séparément. Pour les hôtes ESXi, les règles de pare-feu associent les services avec les pare-feu correspondants et peuvent ouvrir et fermer le pare-feu en fonction de l'état du service. Reportez-vous à « ESXi », page 67.

Vous pouvez également ouvrir explicitement des ports sur les instances de Platform Services Controller et vCenter Server. Reportez-vous aux sections « Ports requis pour vCenter Server et l'instance de Platform Services Controller », page 114 et « Ports TCP et UDP supplémentaires pour vCenter Server », page 119.

Envisager des stratégies de sécurité du réseau

Les stratégies de sécurité du réseau assurent la protection du trafic contre l'emprunt d'identité d'adresse MAC et l'analyse des ports indésirables. La règle de sécurité d'un commutateur standard ou distribué est mise en œuvre au niveau de la couche 2 (couche de liaison de données) de la pile de protocole réseau. Les trois éléments de la stratégie de sécurité sont le mode promiscuité, les changements d'adresse MAC et les Transmissions forgées.

Les instructions sont disponibles dans la documentation *Mise en réseau vSphere*.

Sécuriser la mise en réseau des machines virtuelles

Les méthodes utilisées pour sécuriser le réseau de machines virtuelles dépendent du système d'exploitation invité qui est installé, du fonctionnement des machines virtuelles dans un environnement sécurisé ou non et d'autres facteurs. Les commutateurs virtuels et les commutateurs virtuels distribués offrent un niveau de protection élevé lorsqu'ils sont utilisés avec d'autres mesures de sécurité courantes (installation de pare-feu, notamment).

Reportez-vous à Chapitre 8, « Sécurisation de la mise en réseau vSphere », page 163.

Envisager les VLAN pour protéger votre environnement

ESXi prend en charge les VLAN IEEE 802.1q. Vous pouvez donc les utiliser pour renforcer la protection du réseau de machines virtuelles ou la configuration de stockage. Les VLAN vous permettent de segmenter un réseau physique. Lorsque des VLAN sont utilisés, deux machines sur le même réseau physique ne peuvent pas s'envoyer mutuellement des paquets ni en recevoir, sauf s'ils se trouvent sur le même réseau VLAN.

Reportez-vous à « Sécurisation des machines virtuelles avec des VLAN », page 172.

Sécuriser les connexions du stockage virtualisé

Une machine virtuelle stocke les fichiers du système d'exploitation, les fichiers de programme et d'autres données sur un disque virtuel. Chaque disque virtuel apparaît sur la machine virtuelle en tant que lecteur SCSI connecté au contrôleur SCSI. Une machine virtuelle n'a pas accès aux détails du stockage ni aux informations relatives au LUN sur lequel réside son disque virtuel.

Le système VMFS (Virtual Machine File System) combine un système de fichiers distribué et un gestionnaire de volumes qui présente les volumes virtuels à l'hôte ESXi. La sécurisation de la connexion avec le stockage relève de votre responsabilité. Par exemple, si vous utilisez un stockage iSCSI, vous pouvez configurer votre environnement pour qu'il utilise l'authentification CHAP et, si la stratégie de l'entreprise l'exige, l'authentification CHAP mutuelle, à l'aide de vSphere Web Client ou d'interfaces de ligne de commande.

Reportez-vous à « Meilleures pratiques en matière de sécurité du stockage », page 188.

Évaluer l'utilisation d'IPSec

ESXi prend en charge IPSec sur IPv6. Vous ne pouvez pas utiliser IPSec sur IPv4.

Reportez-vous à « Sécurité du protocole Internet », page 176.

De plus, déterminez si VMware NSX for vSphere est une solution adéquate pour sécuriser la couche de mise en réseau dans votre environnement.

Mots de passe dans votre environnement vSphere

Les restrictions de mot de passe, le verrouillage et l'expiration dans votre environnement vSphere dépendent de plusieurs facteurs : système visé par l'utilisateur, identité de l'utilisateur et mode de définition des règles.

Mots de passe d' ESXi

Les restrictions de mot de passe ESXi sont déterminées par le module PAM Linux pam_passwdqc. Pour le module pam_passwdqc, reportez-vous à la page du manuel Linux et à « Verrouillage des mots de passe et des comptes ESXi », page 45.

Mots de passe pour vCenter Server et autres services de vCenter

vCenter Single Sign-On gère l'authentification pour tous les utilisateurs qui se connectent à vCenter Server et à d'autres services de vCenter. Les restrictions de mot de passe, le verrouillage et l'expiration dépendent du domaine de l'utilisateur et de l'identité de l'utilisateur.

Administrateur de vCenter Single Sign-On

Le mot de passe de l'administrateur vCenter Single Sign-On est administrator@vsphere.local par défaut ou administrator@*mydomain* si vous avez spécifié un domaine différent lors de l'installation. Ce mot de passe n'expire pas. À tous les autres niveaux, le mot de passe doit respecter les restrictions définies dans la stratégie de mot de passe vCenter Single Sign-On. Consultez *Administration de Platform Services Controller* pour plus d'informations.

Si vous oubliez le mot de passe de cet utilisateur, recherchez dans le système de la base de connaissances VMware des informations sur la réinitialisation de ce mot de passe. Pour réinitialiser le mot de passe, des privilèges supplémentaires comme un accès racine sont nécessaires pour accéder au système vCenter Server.

Autres utilisateurs du domaine Single Sign-On vCenter

Les mots de passe des autres utilisateurs vsphere.local ou des utilisateurs du domaine que vous avez spécifiés au cours de l'installation doivent respecter les restrictions définies par la stratégie de mot de passe et la stratégie de verrouillage de vCenter Single Sign-On. Consultez *Administration de Platform Services Controller* pour plus d'informations. Ces mots de passe expirent après 90 jours par défaut, bien que les administrateurs puissent modifier l'expiration dans le cadre de la stratégie de mot de passe.

Si vous oubliez votre mot de passe vsphere.local, un administrateur peut réinitialiser ce mot de passe à l'aide de la commande `dir-cli`.

Autres utilisateurs

Les restrictions de mot de passe, le verrouillage et l'expiration de tous les autres utilisateurs sont déterminés par le domaine (source d'identité) auprès duquel l'utilisateur peut s'authentifier.

vCenter Single Sign-On prend en charge une source d'identité par défaut et les utilisateurs peuvent se connecter au domaine correspondant à vSphere Web Client simplement avec leur nom d'utilisateur. Si des utilisateurs veulent se connecter à un domaine qui n'est pas le domaine par défaut, ils peuvent inclure le nom de domaine, c'est-à-dire spécifier *utilisateur@domaine* ou *domaine\utilisateur*. Les paramètres de mot de passe d'accès au domaine s'appliquent à chaque domaine.

Mots de passe pour les utilisateurs de l'interface utilisateur de la console directe de vCenter Server Appliance

vCenter Server Appliance est une machine virtuelle basée sur Linux préconfigurée et optimisée pour l'exécution de vCenter Server et des services associés sur Linux.

Lorsque vous déployez le dispositif vCenter Server Appliance, vous devez spécifier ces mots de passe.

- Mot de passe de l'utilisateur racine du système d'exploitation Linux du dispositif.
- Mot de passe de l'administrateur du domaine vCenter Single Sign-On, administrator@vsphere.local par défaut.

Vous pouvez modifier le mot de passe de l'utilisateur racine et effectuer d'autres tâches de gestion d'utilisateur local du dispositif vCenter Server Appliance depuis la console de celui-ci. Voir *Configuration de vCenter Server Appliance*.

Meilleures pratiques en matière de sécurité et ressources de sécurité

Si vous suivez les meilleures pratiques, votre ESXi et vCenter Server peuvent être au moins aussi sûr qu'un environnement non virtualisé.

Ce manuel répertorie les meilleures pratiques pour les différents composants de votre infrastructure vSphere.

Tableau 1-1. Meilleures pratiques de sécurité

Composant de vSphere	Ressource
hôte ESXi	Chapitre 3, « Sécurisation des hôtes ESXi », page 41
Système vCenter Server	« Meilleures pratiques de sécurité de vCenter Server », page 107
Machine virtuelle	« Recommandations en matière de sécurité des machines virtuelles », page 124
Mise en réseau vSphere	« Meilleures pratiques en matière de sécurité de la mise en réseau vSphere », page 180

Ce manuel ne représente que l'une des sources dont vous avez besoin pour assurer la sécurité de l'environnement.

Les ressources de sécurité VMware, notamment les alertes et les téléchargements de sécurité, sont disponibles en ligne.

Tableau 1-2. Ressources de sécurité VMware disponibles sur le Web

Rubrique	Ressource
Stratégie de sécurité VMware, alertes de sécurité à jour, téléchargements de sécurité et discussions sur des thèmes liés à la sécurité.	http://www.vmware.com/go/security
Politique de l'entreprise en matière de réponse sécuritaire	http://www.vmware.com/support/policies/security_response.html VMware s'engage à vous aider à maintenir un environnement sécurisé. Dans ce cadre, les problèmes de sécurité sont corrigés rapidement. La politique VMware en matière de réponse sécuritaire fait état de notre engagement lié à la résolution d'éventuelles vulnérabilités de nos produits.

Tableau 1-2. Ressources de sécurité VMware disponibles sur le Web (suite)

Rubrique	Ressource
Politique de support logiciel tiers	http://www.vmware.com/support/policies/ VMware prend en charge un grand nombre de systèmes de stockage et d'agents logiciels (tels que les agents de sauvegarde ou les agents de gestion système). Vous trouverez la liste des agents, outils et autres logiciels prenant en charge ESXi en cherchant sur http://www.vmware.com/vmtn/resources/ les guides de compatibilité ESXi. Il existe sur le marché un nombre de produits et de configurations tel quel VMware ne peut pas tous les tester. Si un produit ou une configuration spécifique ne figure pas dans l'un des guides de compatibilité, contactez le Support technique, qui pourra vous aider à résoudre les problèmes rencontrés ; en revanche, il ne pourra pas vous garantir que ce produit ou cette configuration peut être utilisé. Vous devez toujours évaluer les risques de sécurité liés aux produits ou aux configurations non pris en charge.
Standards de sécurité et de conformité, ainsi que solutions partenaires et contenu détaillé sur la virtualisation et la conformité	http://www.vmware.com/go/compliance
Informations sur les certifications et les validations de sécurité telles que CCEVS et FIPS pour les différentes versions des composants de vSphere.	https://www.vmware.com/support/support-resources/certifications.html
Guides de sécurisation renforcée pour les différentes versions de vSphere et d'autres produits VMware.	https://www.vmware.com/support/support-resources/hardening-guides.html
Livre blanc *Sécurité de VMware vSphere Hypervisor*	http://www.vmware.com/files/pdf/techpaper/vmw-wp-secrty-vsphr-hyprvsr-uslet-101.pdf

Tâches de gestion des utilisateurs et des autorisations de vSphere 2

L'authentification et l'autorisation gouvernent l'accès. vCenter Single Sign-On prend en charge l'authentification, ce qui signifie qu'il détermine si un utilisateur peut accéder à l'intégralité des composants vSphere ou pas. Chaque utilisateur doit également être autorisé à afficher ou à manipuler des objets vSphere.

vSphere prend en charge différents mécanismes d'autorisation abordés dans « Présentation des autorisations dans vSphere », page 20. Cette section aborde essentiellement le fonctionnement du modèle d'autorisation vCenter Server et le mode d'exécution des tâches de gestion des utilisateurs.

vCenter Server permet un contrôle plus complet des permissions en général grâce aux autorisations et aux rôles. Lorsque vous attribuez une autorisation à un objet de la hiérarchie d'objets de vCenter Server, vous spécifiez les privilèges dont l'utilisateur ou le groupe dispose sur cet objet. Pour spécifier les privilèges, vous utilisez des rôles, qui sont des ensembles de privilèges.

À l'origine, seul l'administrateur du domaine vCenter Single Sign-On, administrator@vsphere.local par défaut, est autorisé à se connecter au système vCenter Server. Cet utilisateur peut alors procéder comme suit :

1. Ajouter une source d'identité dans laquelle les utilisateurs et les groupes sont définis sur vCenter Single Sign-On. Consultez la documentation de *Administration de Platform Services Controller* .
2. Accordez des privilèges à un utilisateur ou à un groupe en sélectionnant un objet tel qu'une machine virtuelle ou un système vCenter Server et en attribuant un rôle de cet objet à l'utilisateur ou au groupe.

Rôles, privilèges et autorisations (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_roles_privileges_permissions_vsphere_web_client)

Ce chapitre aborde les rubriques suivantes :

Présentation des autorisations dans vSphere

Vous autorisez un utilisateur ou un groupe d'utilisateurs à effectuer des tâches sur les objets vCenter en utilisant des autorisations sur l'objet.

vSphere 6.0 et versions ultérieures permet à des utilisateurs privilégiés d'accorder à d'autres utilisateurs des autorisations d'exécution de tâches des manières suivantes. Ces approches s'excluent mutuellement dans la plupart des cas. Cependant, vous pouvez attribuer l'utilisation d'autorisations globales pour autoriser certains utilisateurs pour toutes les solutions, et des autorisations vCenter Server locales pour autoriser les autres utilisateurs pour les instances de vCenter Server individuelles.

Autorisations vCenter Server

Le modèle d'autorisation des systèmes vCenter Server repose sur l'attribution d'autorisations à des objets dans la hiérarchie d'objets. Chaque autorisation accorde à un utilisateur ou à un groupe un ensemble de privilèges, c'est-à-dire un rôle sur l'objet sélectionné. Par exemple, vous pouvez sélectionner un hôte ESXi dans la hiérarchie d'objets et attribuer un rôle à un groupe d'utilisateurs pour attribuer à ces utilisateurs les privilèges correspondants sur cet hôte.

Autorisations globales

Les autorisations globales sont appliquées à un objet racine global qui peut couvrir plusieurs solutions à la fois. Par exemple, si vCenter Server et vRealize Orchestrator sont installés, vous pouvez utiliser des autorisations locales pour attribuer à un groupe d'utilisateurs des autorisations de lecture sur tous les objets dans les deux hiérarchies d'objets.

Les autorisations globales sont répliquées dans le domaine vsphere.local. Les autorisations globales ne fournissent pas d'autorisations pour les services gérés via des groupes vsphere.local. Reportez-vous à « Autorisations globales », page 30.

Appartenance à un groupe dans les groupes vsphere.local

L'utilisateur du domaine vCenter Single Sign-On (administrator@vsphere.local par défaut), peut effectuer les tâches qui sont associées aux services inclus avec Platform Services Controller. Les membres d'un groupe vsphere.local peuvent effectuer certaines tâches. Par exemple, vous pouvez effectuer la gestion de licences si vous êtes membre du groupe LicenseService.Administrators. Consultez la documentation de *Administration de Platform Services Controller* .

Autorisations d'hôte ESXi local

Si vous gérez un système ESXi autonome qui n'est pas géré par un système vCenter Server, vous pouvez attribuer l'un des rôles prédéfinis aux utilisateurs. Consultez la documentation de *Gestion individuelle des hôtes vSphere - VMware Host Client*.

Pour les hôtes gérés, attribuez des rôles à l'objet hôte ESXi dans l'inventaire vCenter Server.

Présentation du modèle d'autorisation vCenter Server

Le modèle d'autorisation des systèmes vCenter Server repose sur l'attribution d'autorisations à des objets dans la hiérarchie d'objets vSphere. Chaque autorisation accorde un ensemble de privilèges à un utilisateur ou à un groupe, c'est-à-dire un rôle pour l'objet sélectionné.

Les concepts suivants sont importants.

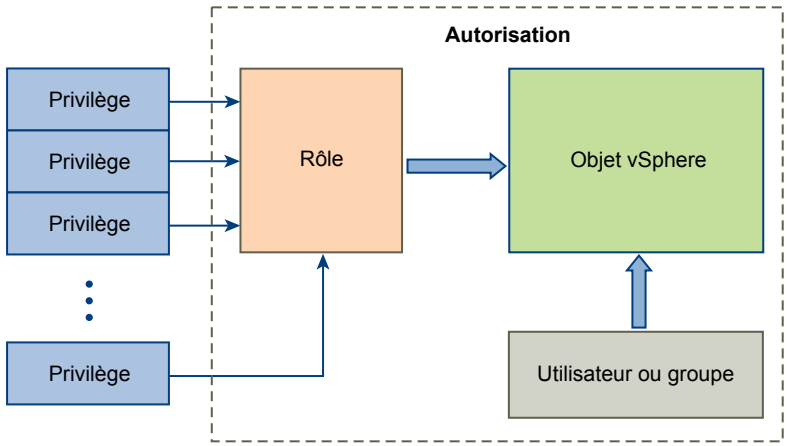
Autorisations Chaque objet de la hiérarchie des objets vCenter Server a des autorisations associées. Chaque autorisation spécifie pour un groupe ou un utilisateur les privilèges dont dispose ce groupe ou cet utilisateur sur l'objet.

Utilisateurs et groupes Sur les systèmes vCenter Server, vous ne pouvez attribuer des privilèges qu'aux utilisateurs ou aux groupes d'utilisateurs authentifiés. Les utilisateurs sont authentifiés via vCenter Single Sign-On. Les utilisateurs et les groupes doivent être définis dans la source d'identité utilisée par vCenter Single Sign-On pour l'authentification. Définissez les utilisateurs et les groupes à l'aide des outils de votre source d'identité, par exemple Active Directory.

Privilèges Les privilèges sont des contrôles d'accès précis. Vous pouvez regrouper ces privilèges dans des rôles, que vous pouvez ensuite mapper à des utilisateurs ou à des groupes.

Rôles Les rôles sont des ensembles de privilèges. Les rôles vous permettent d'attribuer des autorisations sur un objet en fonction d'un ensemble de tâches par défaut exécutées par les utilisateurs. Les rôles par défaut, par exemple Administrateur, sont prédéfinis sur vCenter Server et ne peuvent pas être modifiés. D'autres rôles, par exemple Administrateur de pool de ressources, sont des exemples de rôles prédéfinis. Vous pouvez créer des rôles personnalisés totalement nouveaux, ou cloner et modifier des exemples de rôles. Reportez-vous aux sections « Créer un rôle personnalisé », page 35 et « Cloner un rôle », page 35.

Figure 2-1. Autorisations de vSphere



Pour attribuer des autorisations à un objet, suivez les étapes suivantes :

1 Sélectionnez l'objet auquel vous souhaitez appliquer l'autorisation dans la hiérarchie des objets vCenter.

2 Sélectionnez le groupe ou l'utilisateur qui doit avoir des privilèges sur l'objet.

3 Sélectionnez des privilèges individuels ou un rôle, c'est-à-dire un ensemble de privilèges, que le groupe ou l'utilisateur doit avoir sur l'objet.

   Par défaut, les autorisations se propagent, c'est-à-dire que le groupe ou l'utilisateur a le rôle sélectionné sur l'objet sélectionné et ses objets enfants.

Le modèle d'autorisations permet d'accélérer la réalisation des tâches en offrant des rôles prédéfinis. Vous pouvez également créer des rôles personnalisés en combinant. Voir Chapitre 10, « Privilèges définis », page 193 pour obtenir une référence à l'ensemble des privilèges et aux objets auxquels vous pouvez appliquer les privilèges. Voir « Privilèges requis pour les tâches courantes », page 37 pour consulter des exemples d'ensembles de privilèges requis pour effectuer des tâches courantes.

Les autorisations doivent souvent être définies à la fois sur un objet source et un objet de destination. Par exemple, si vous déplacez une machine virtuelle, vous devez disposer de privilèges sur cette machine virtuelle ainsi que sur le centre de données de destination.

Le modèle d'autorisations des hôtes ESXi autonomes est plus simple. Reportez-vous à « Attribution de privilèges pour les hôtes ESXi », page 84.

Validation des utilisateurs de vCenter Server

Les systèmes vCenter Server qui utilisent régulièrement un service d'annuaire valident les utilisateurs et les groupes selon le domaine de l'annuaire utilisateur. La validation est effectuée à intervalles réguliers, comme spécifié dans les paramètres de vCenter Server. Par exemple, supposez qu'un rôle soit attribué à l'utilisateur Smith sur plusieurs objets. L'administrateur de domaine modifie le nom en Smith2. L'hôte conclut que Smith n'existe plus et supprime les autorisations associées à cet utilisateur à partir des objets vSphere lors de la prochaine validation.

De même, si l'utilisateur Smith est supprimé du domaine, toutes les autorisations associées à cet utilisateur sont supprimées lors de la validation suivante. Si un nouvel utilisateur Smith est ajouté au domaine avant la validation suivante, les autorisations des objets de l'ancien utilisateur Smith sont remplacées par celles du nouvel utilisateur Smith.

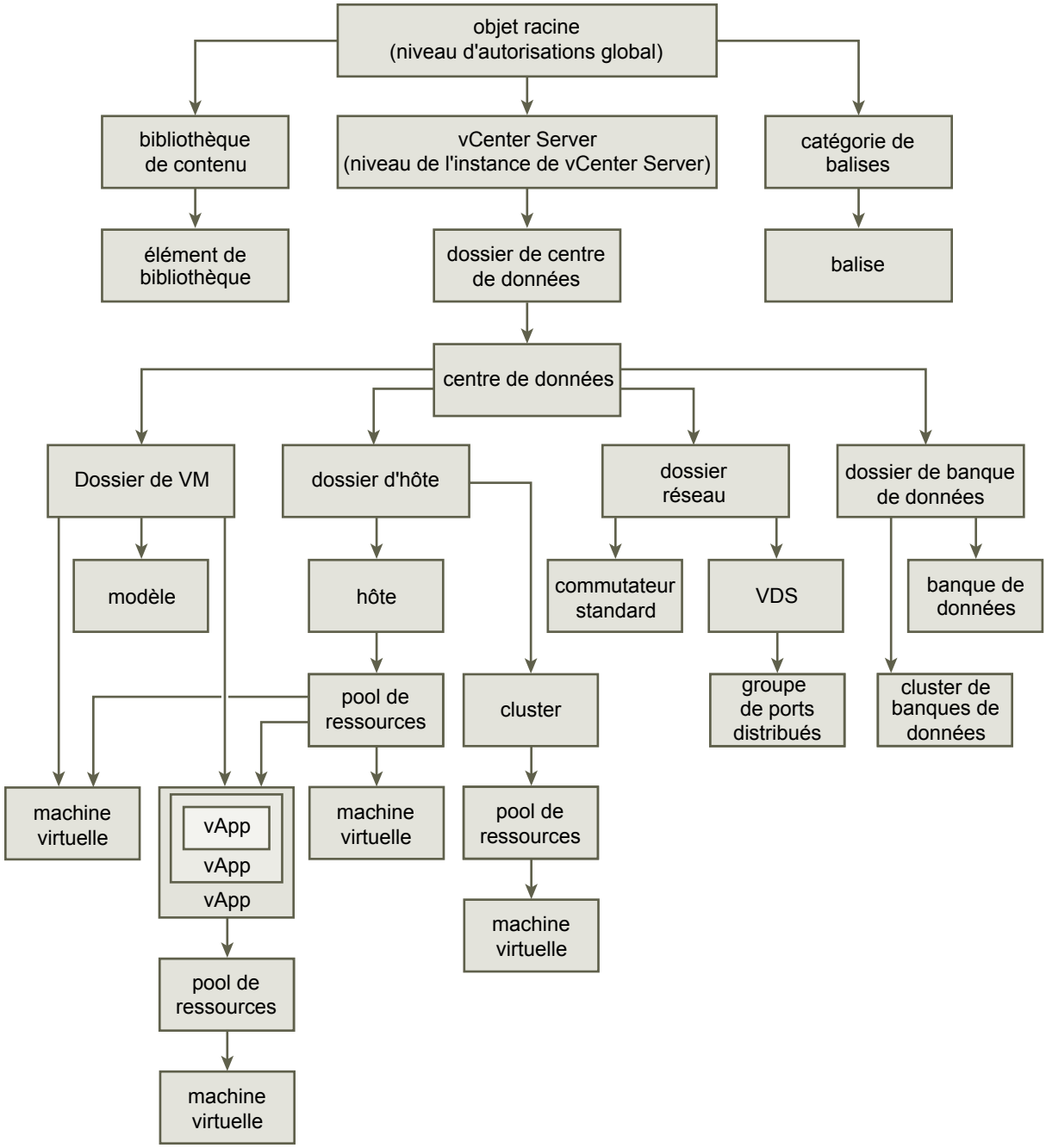
Héritage hiérarchique des autorisations

Quand vous assignez une autorisation à un objet, vous pouvez choisir si l'autorisation propage la hiérarchie d'objet. Vous définissez la propagation pour chaque autorisation. La propagation n'est pas universellement appliquée. Les autorisations définies pour un objet enfant ignorent toujours les autorisations qui sont propagées à partir des objets parent.

La figure illustre la hiérarchie d'inventaire et les chemins par lesquels les autorisations peuvent être propagées.

Remarque Les autorisations globales prennent en charge l'attribution de privilèges dans plusieurs solutions à partir d'un objet racine global. Reportez-vous à « Autorisations globales », page 30.

Figure 2-2. Hiérarchie d'inventaire de vSphere



La plupart des objets d'inventaire héritent des autorisations d'un objet parent unique dans la hiérarchie. Par exemple, un centre de données hérite des autorisations de son dossier parent du centre de données ou du centre de données de parent. Les machines virtuelles héritent des autorisations du dossier parent de machine virtuelle et simultanément l'hôte, le cluster ou le pool de ressources parent.

Par exemple, pour définir des autorisations pour un Distributed Switch et ses groupes de ports distribués associés, définissez les autorisations sur un objet parent, tel qu'un dossier ou un centre de données. Vous devez également sélectionner l'option pour propager ces autorisations aux objets enfant.

Les autorisations prennent plusieurs formes dans la hiérarchie :

Entités gérées

Les utilisateurs privilégiés peuvent définir des autorisations sur des entités gérées.

- Clusters
- Centres de données
- Banques de données
- Clusters de banques de données
- Dossiers
- Hôtes
- Réseaux (excepté vSphere Distributed Switches)
- Groupes de ports distribués
- Pools de ressources
- Modèles
- Machines virtuelles
- vSphere vApps

Entités globales

Vous ne pouvez pas modifier les autorisations sur des entités qui dérivent les autorisations du système vCenter Server racine.

- Champs personnalisés
- Licences
- Rôles
- Intervalles de statistiques
- Sessions

Paramètres d'autorisation multiples

Les objets peuvent avoir des autorisations multiples, mais seulement une autorisation pour chaque utilisateur ou groupes. Par exemple, une autorisation peut spécifier que le groupe B dispose des privilèges d'administrateur sur l'objet, et une autre autorisation peut spécifier que le groupe B peut disposer de privilèges d'administrateur de machine virtuelle sur le même objet.

Si un objet hérite des autorisations de deux objets parents, les autorisations d'un objet sont ajoutées à celles de l'autre objet. Par exemple, si une machine virtuelle se trouve dans un dossier de machine virtuelle et appartient également à un pool de ressources, cette machine virtuelle hérite de tous les paramètres d'autorisation du dossier de la machine virtuelle et de ceux du pool de ressources.

Les autorisations appliquées sur un objet enfant ignorent toujours les autorisations qui sont appliquées sur un objet parent. Reportez-vous à « Exemple 2 : Autorisations d'enfant ignorant des autorisations de parent », page 25.

Si des autorisations multiples de groupes sont définies sur le même objet et qu'un utilisateur appartient à au moins deux de ces groupes, deux situations sont possibles :

- Si aucune autorisation n'est définie pour l'utilisateur sur cet objet, l'ensemble de privilèges assignés aux groupes pour cet objet est assigné à l'utilisateur.
- Si une autorisation est définie pour l'utilisateur sur cet objet, l'autorisation de l'utilisateur a la priorité sur toutes les autorisations de groupes.

Exemple 1 : Héritage d'autorisations multiples

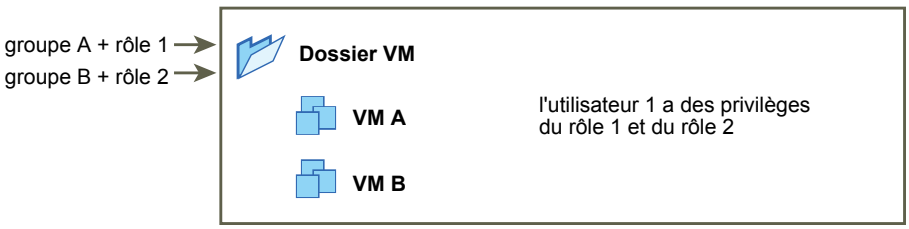
Cet exemple illustre comment un objet peut hériter d'autorisations multiples de groupes auxquels ont été accordés l'autorisation sur un objet parent.

Dans cet exemple, deux autorisations sont assignées sur le même objet pour deux groupes différents.

- Le rôle 1 peut mettre des machines virtuelles sous tension.
- Le rôle 2 peut prendre des snapshots de machines virtuelles.
- On accorde au groupes A le rôle 1 sur le dossier de VM, avec l'autorisation définie pour propager aux objets enfant.
- On accorde au groupes B le rôle 2 sur le dossier de VM, avec l'autorisation définie pour propager aux objets enfant.
- Aucun privilège spécifique n'est attribué à l'utilisateur 1.

L'utilisateur 1, qui appartient aux groupes A et B, se connecte. L'utilisateur 1 peut mettre sous tension et prendre des snapshots de VM A et de VM B.

Figure 2-3. Exemple 1 : Héritage d'autorisations multiples



Exemple 2 : Autorisations d'enfant ignorant des autorisations de parent

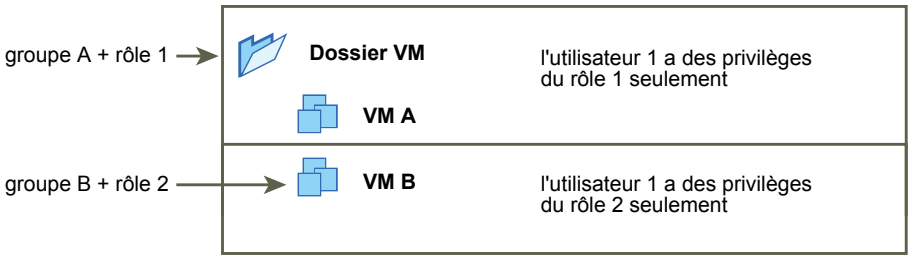
Cet exemple illustre comment les autorisations qui sont assignées sur un objet enfant peuvent ignorer les autorisations qui sont assignées sur un objet parent. Vous pouvez utiliser ce comportement de non prise en compte pour limiter l'accès client à des zones spécifiques de l'inventaire.

Dans cet exemple, des autorisations sont définies sur deux objets différents pour deux groupes différents.

- Le rôle 1 peut mettre des machines virtuelles sous tension.
- Le rôle 2 peut prendre des snapshots de machines virtuelles.
- On accorde au groupes A le rôle 1 sur le dossier de VM, avec l'autorisation définie pour propager aux objets enfant.
- On accorde le groupes B le rôle 2 sur VM B.

L'utilisateur 1, qui appartient aux groupes A et B, se connecte. Puisque le rôle 2 est assigné à un point inférieur dans la hiérarchie que le rôle 1, il ignore le rôle 1 sur VM B. L'utilisateur 1 peut mettre sous tension VM A, mais ne peut pas prendre des snapshots. L'utilisateur 1 peut prendre des snapshots de VM B, mais ne peut pas les mettre sous tension.

Figure 2-4. Exemple 2 : Autorisations d'enfant ignorant des autorisations de parent



Exemple 3 : Rôle d'utilisateur supprimant un rôle de groupe

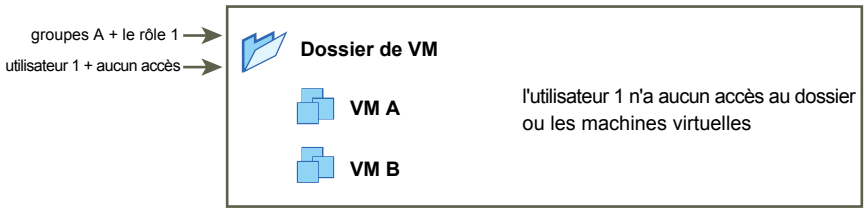
Cet exemple illustre comment le rôle attribué directement à un utilisateur individuel remplace les privilèges associés à un rôle attribué à un groupe.

Dans cet exemple, les autorisations sont définies sur le même objet. Une autorisation associe un groupe à un rôle et l'autre l'autorisation associe un utilisateur individuel à un rôle. L'utilisateur est un membre du groupe.

- Le rôle 1 peut mettre des machines virtuelles sous tension.
- On accorde au groupes A le rôle 1 sur le dossier de VM.
- On accorde à l'utilisateur 1 un rôle Aucun accès sur le dossier de VM.

L'utilisateur 1, qui appartient au groupes A, se connecte. Le rôle Aucun accès accordé à l'utilisateur 1 sur le dossier de VM remplace le rôle attribué au groupe. L'utilisateur 1 n'a aucun accès au dossier ou aux VM A et B. de VM.

Figure 2-5. Exemple 3 : Autorisations d'utilisateurs ignorant des autorisations de groupes



Gestion des autorisations des composants vCenter

Une autorisation est définie sur une hiérarchie d'objets vCenter. Chaque autorisation associe l'objet à un groupe ou un utilisateur et aux rôles d'accès correspondants. Par exemple, vous pouvez sélectionner un objet de machine virtuelle, ajouter une autorisation qui accorde le rôle en lecture seule au Groupe 1 et ajouter une deuxième autorisation qui accorde le rôle d'administrateur à l'utilisateur 2.

En attribuant un rôle différent à un groupe d'utilisateurs sur différents objets, vous contrôlez les tâches que les utilisateurs peuvent effectuer dans votre environnement vSphere. Par exemple, pour autoriser un groupe à configurer la mémoire de l'hôte, sélectionnez l'hôte et ajoutez une autorisation qui accorde à ce groupe un rôle incluant le privilège **Hôte.Configuration.Configuration mémoire**.

Pour gérer les autorisations de vSphere Web Client, vous devez comprendre les concepts suivants :

Autorisations Chaque objet de la hiérarchie des objets vCenter Server a des autorisations associées. Chaque autorisation spécifie pour un groupe ou un utilisateur les privilèges dont dispose ce groupe ou cet utilisateur sur l'objet.

Utilisateurs et groupes Sur les systèmes vCenter Server, vous ne pouvez attribuer des privilèges qu'aux utilisateurs ou aux groupes d'utilisateurs authentifiés. Les utilisateurs sont authentifiés via vCenter Single Sign-On. Les utilisateurs et les groupes doivent être définis dans la source d'identité utilisée par vCenter Single Sign-On pour l'authentification. Définissez les utilisateurs et les groupes à l'aide des outils de votre source d'identité, par exemple Active Directory.

Privilèges Les privilèges sont des contrôles d'accès précis. Vous pouvez regrouper ces privilèges dans des rôles, que vous pouvez ensuite mapper à des utilisateurs ou à des groupes.

Rôles Les rôles sont des ensembles de privilèges. Les rôles vous permettent d'attribuer des autorisations sur un objet en fonction d'un ensemble de tâches par défaut exécutées par les utilisateurs. Les rôles par défaut, par exemple Administrateur, sont prédéfinis sur vCenter Server et ne peuvent pas être modifiés. D'autres rôles, par exemple Administrateur de pool de ressources, sont des exemples de rôles prédéfinis. Vous pouvez créer des rôles personnalisés totalement nouveaux, ou cloner et modifier des exemples de rôles. Reportez-vous aux sections « Créer un rôle personnalisé », page 35 et « Cloner un rôle », page 35.

Vous pouvez attribuer des autorisations à des objets sur différents niveaux de la hiérarchie. Vous pouvez, par exemple, attribuer des autorisations à un objet d'hôte ou de dossier qui inclut tous les objets d'hôte. Reportez-vous à « Héritage hiérarchique des autorisations », page 22. Vous pouvez également attribuer des autorisations à un objet racine global pour appliquer les autorisations à l'ensemble des objets dans toutes les solutions. Reportez-vous à « Autorisations globales », page 30.

Ajouter une autorisation à un objet d'inventaire

Après avoir créé des utilisateurs et des groupes et avoir défini des rôles, vous devez affecter les utilisateurs et les groupes et leurs rôles aux objets appropriés d'inventaire. Vous pouvez attribuer les mêmes autorisations à plusieurs objets en même temps en déplaçant les objets vers un dossier et en définissant les autorisations du dossier.

Lorsque vous attribuez des autorisations dans vSphere Web Client, les noms des utilisateurs et des groupes doivent correspondre exactement à ceux d'Active Directory, y compris la casse. Si vous avez effectué une mise à niveau à partir de versions antérieures de vSphere, vérifiez le respect de la casse si vous rencontrez des problèmes avec les groupes.

Prérequis

Le rôle qui vous est attribué sur l'objet dont vous souhaitez modifier les autorisations doit inclure le privilège **Autorisations.Modifier autorisation**.

Procédure

1. Accédez à l'objet auquel vous souhaitez attribuer des autorisations dans le navigateur d'objets de vSphere Web Client.
2. Cliquez sur l'onglet **Autorisations**.
3. Cliquez sur l'icône Ajouter, puis cliquez sur **Ajouter**.

4 Sélectionnez l'utilisateur ou le groupe qui disposera des privilèges définis par le rôle sélectionné.

   a Dans le menu déroulant **Domaine**, sélectionnez le domaine où se trouve l'utilisateur ou le groupe.

   b Entrez un nom dans la fenêtre de recherche ou sélectionnez un nom dans la liste.

   Le système recherche des noms d'utilisateur, des noms de groupe et des descriptions.

   c Sélectionnez l'utilisateur ou le groupe, puis cliquez sur **Ajouter**.

   Le nom est ajouté soit à la liste **Utilisateurs** soit à la liste **groupes**.

   d (Facultatif) Cliquez sur **Vérifier les noms** pour vérifier que l'utilisateur ou le groupe existe dans la source d'identité.

   e Cliquez sur **OK**.

5 Sélectionner un rôle du menu déroulant **Rôle assigné**.

   Les rôles qui sont attribués à l'objet apparaissent dans le menu. Les privilèges contenus dans le rôle sont mentionnés dans la section au-dessous de l'intitulé du rôle.

6 (Facultatif) Pour limiter la propagation, décochez la case **Propager vers les objets enfants**.

   Le rôle est appliqué seulement à l'objet sélectionné et ne se propage pas aux objets enfant.

7 Cliquez sur **OK** pour ajouter l'autorisation.

Changer des autorisations

Après avoir défini un utilisateur ou un groupe et une paire de rôle pour un objet d'inventaire, vous pouvez changer le rôle apparié avec l'utilisateur ou le groupes ou changer le paramètre de la case à cocher **Propager**. Vous pouvez également supprimer le paramètre d'autorisation.

Procédure

1 Accédez à l'objet dans le navigateur d'objets de vSphere Web Client.

2 Cliquez sur l'onglet **Autorisations**.

3 Cliquez sur une ligne pour sélectionner une autorisation.

4 Cliquez sur l'icône **Modifier un rôle dans l'autorisation**.

5 Sélectionnez un rôle pour l'utilisateur ou le groupe dans le menu déroulant **Rôle assigné**.

6 Cochez/décochez la case **Propager vers les enfants** pour modifier l'héritage d'autorisations et cliquez sur **OK**.

Supprimer les autorisations

Vous pouvez supprimer des autorisations sur un objet de la hiérarchie d'objets, pour un utilisateur spécifique ou pour un groupe d'utilisateurs. Dans ce cas, l'utilisateur ou le groupe ne dispose plus des privilèges associés au rôle défini sur l'objet.

Remarque Vous ne pouvez pas supprimer les autorisations qui sont prédéfinies par le système.

Procédure

1 Accédez à l'objet dans le navigateur d'objets de vSphere Web Client.

2 Cliquez sur l'onglet **Configurer** et sélectionnez **Autorisations**.

3 Cliquez sur une ligne pour sélectionner une autorisation.

4 Cliquez sur l'icône **Supprimer autorisation**.

Changer les paramètres de validation d'utilisateur

vCenter Server valide périodiquement ses listes d'utilisateurs et de groupes selon les utilisateurs et les groupes figurant dans l'annuaire d'utilisateurs. Il supprime alors les utilisateurs ou les groupes qui n'existent plus dans le domaine. Vous pouvez désactiver la validation ou modifier l'intervalle entre les validations. Si vos domaines comportent des milliers de groupes ou d'utilisateurs, ou si les recherches prennent trop de temps, envisagez d'ajuster les paramètres de recherche.

Pour les versions de vCenter Server antérieures à vCenter Server 5.0, ces paramètres s'appliquent à un Active Directory associé à vCenter Server. Pour vCenter Server 5.0 et versions ultérieures, ces paramètres s'appliquent aux sources d'identité de vCenter Single Sign-On.

Remarque Cette procédure s'applique uniquement aux listes d'utilisateurs de vCenter Server. Vous ne pouvez pas faire des recherches dans les listes d'utilisateurs de ESXi de la même façon.

Procédure

1 Accédez au système vCenter Server dans le navigateur d'objets de vSphere Web Client.

2 Sélectionnez **Configurer** et cliquez sur **Général** dans la section **Paramètres**.

3 Cliquez sur **Modifier** et sélectionnez **Répertoire de l'utilisateur**.

4 Modifiez les valeurs si nécessaire.

Option	Description
Délai d'expiration de l'annuaire d'utilisateurs	Délai d'expiration en secondes pour la connexion au serveur Active Directory. Cette valeur spécifie le délai maximal pendant lequel vCenter Server autorise l'exécution de la recherche sur le domaine sélectionné. La recherche dans de grands domaines peut prendre du temps.
Limite de requête	Cochez cette case pour définir le nombre maximal d'utilisateurs et de groupes qui s'affichent dans vCenter Server.
Taille limite de requête	Nombre maximal d'utilisateurs et de groupes du domaine sélectionné que vCenter Server affiche dans la boîte de dialogue **Choisir les utilisateurs ou les groupes**. Si vous entrez 0 (zéro), tous les utilisateurs et groupes apparaissent.
Validation	Décochez cette case pour désactiver la validation
Période de validation	Spécifie combien de fois vCenter Server valide les autorisations, en minutes.

5 Cliquez sur **OK**.

Autorisations globales

Les autorisations globales sont appliquées à un objet racine global qui peut couvrir plusieurs solutions à la fois (vCenter Server et vRealize Orchestrator, par exemple). Utilisez les autorisations globales pour accorder à un utilisateur ou à un groupe des privilèges pour tous les objets dans l'ensemble des hiérarchies d'objets.

Un objet racine se trouve dans la hiérarchie d'objets de chaque solution. L'objet racine global agit comme un objet parent des objets racine pour toutes les solutions. Vous pouvez attribuer des autorisations globales à des utilisateurs ou des groupes et choisir le rôle de chaque utilisateur ou de chaque groupe. Le rôle détermine l'ensemble de privilèges attribués à l'utilisateur ou au groupe pour tous les objets de la hiérarchie. Vous pouvez attribuer un rôle prédéfini ou créer des rôles personnalisés. Reportez-vous à « Utilisation des rôles pour assigner des privilèges », page 32. Il est important de faire la distinction entre les autorisations vCenter Server et les autorisations globales.

Autorisations vCenter Server

Dans la plupart des cas, vous appliquez une autorisation à un vCenter Server objet d'inventaire tel qu'un hôte ESXi ou une machine virtuelle. À ce moment-là, vous spécifiez qu'un utilisateur ou un groupe dispose d'un ensemble de privilèges (appelé « rôle ») sur l'objet.

Autorisations globales

Les autorisations globales accordent à un utilisateur ou à un groupe des privilèges permettant d'afficher ou de gérer tous les objets dans chaque hiérarchie d'inventaire de votre déploiement.

Si vous attribuez une autorisation globale sans sélectionner l'option Propager, les utilisateurs ou les groupes associés à cette autorisation n'ont pas accès aux objets de la hiérarchie. Ils n'ont accès qu'à certaines fonctions globales telles que la création de rôles.

Important Les autorisations globales doivent être utilisées avec précaution. Vérifiez que vous voulez vraiment attribuer des autorisations à tous les objets dans l'ensemble des hiérarchies d'inventaire.

Ajouter une autorisation globale

Vous pouvez utiliser les autorisations globales pour accorder à un utilisateur ou à un groupe des privilèges pour tous les objets dans l'ensemble des hiérarchies d'inventaire de votre déploiement.

Important Les autorisations globales doivent être utilisées avec précaution. Vérifiez que vous voulez vraiment attribuer des autorisations à tous les objets dans l'ensemble des hiérarchies d'inventaire.

Prérequis

Pour effectuer cette tâche, vous devez disposer des privilèges **Autorisations.Modifier autorisation** sur l'objet racine de l'ensemble des hiérarchies d'inventaire.

Procédure

1. Cliquez sur **Administration** et sélectionnez **Autorisations globales** dans la zone Contrôle d'accès.
2. Cliquez sur **Gérer**, puis sur l'icône Ajouter autorisation.
3. Sélectionnez l'utilisateur ou le groupe qui disposera des privilèges définis par le rôle sélectionné.
   a. Dans le menu déroulant **Domaine**, sélectionnez le domaine où se trouve l'utilisateur ou le groupe.
   b. Entrez un nom dans la fenêtre de recherche ou sélectionnez un nom dans la liste.

      Le système recherche des noms d'utilisateur, des noms de groupe et des descriptions.
   c. Sélectionnez l'utilisateur ou le groupe, puis cliquez sur **Ajouter**.

      Le nom est ajouté soit à la liste **Utilisateurs** soit à la liste **groupes**.

d (Facultatif) Cliquez sur **Vérifier les noms** pour vérifier que l'utilisateur ou le groupe existe dans la source d'identité.

e Cliquez sur **OK**.

4 Sélectionner un rôle du menu déroulant **Rôle assigné**.

Les rôles qui sont attribués à l'objet apparaissent dans le menu. Les privilèges contenus dans le rôle sont mentionnés dans la section au-dessous de l'intitulé du rôle.

5 Laissez la case **Propager vers les enfants** cochée dans la plupart des cas.

Si vous attribuez une autorisation globale sans sélectionner l'option **Propager**, les utilisateurs ou les groupes associés à cette autorisation n'ont pas accès aux objets de la hiérarchie. Ils n'ont accès qu'à certaines fonctions globales telles que la création de rôles.

6 Cliquez sur **OK**.

Autorisations sur les objets de balise

Dans la hiérarchie d'objets de vCenter Server, les objets de balise ne sont pas des enfants de vCenter Server mais sont créés au niveau racine de vCenter Server. Dans les environnements avec plusieurs instances de vCenter Server, les objets de balise sont partagés entre les instances de vCenter Server. Dans la hiérarchie d'objets de vCenter Server, les autorisations pour les objets de balise fonctionnent différemment des autorisations pour les autres objets.

Seules les autorisations globales ou attribuées à l'objet de balise s'appliquent

Si vous accordez des autorisations à un utilisateur sur un objet d'inventaire de vCenter Server, comme un hôte ou une machine virtuelle ESXi, l'utilisateur ne peut pas effectuer d'opérations de balisage sur cet objet.

Par exemple, si vous accordez le privilège **Attribuer une balise vSphere** à l'utilisateur Dana sur le TPA de l'hôte, cette autorisation ne modifie pas le droit accordé ou non à Dana de lui attribuer des balises. Dana doit disposer du privilège **Attribuer une balise vSphere** au niveau racine - c'est-à-dire une autorisation globale - ou du privilège pour l'objet de balise.

Tableau 2-1. Conséquences des autorisations globales et des autorisations sur les objets sur ce que peuvent faire les utilisateurs

Autorisation globale	Autorisation au niveau des balises	vCenter Server Autorisation au niveau des objets	Autorisation valable
Aucun privilège de balisage accordé	Dana dispose des privilèges **Attribuer une balise vSphere ou en annuler l'attribution** pour la balise.	Dana dispose des privilèges **Supprimer une balise vSphere** sur le TPA de l'hôte ESXi	Dana dispose des privilèges **Attribuer une balise vSphere ou en annuler l'attribution** pour la balise.
Dana dispose des privilèges **Attribuer une balise vSphere ou en annuler l'attribution**.	Aucun privilège n'est attribué pour la balise.	Dana dispose des privilèges **Supprimer une balise vSphere** sur le TPA de l'hôte ESXi	Dana dispose des privilèges globaux **Attribuer une balise vSphere ou en annuler l'attribution**. Ceci inclut des privilèges au niveau des balises.
Aucun privilège de balisage accordé	Aucun privilège n'est attribué pour la balise.	Dana dispose des privilèges **Attribuer une balise vSphere ou en annuler l'attribution** sur le TPA de l'hôte ESXi	Dana ne dispose des privilèges de balisage sur aucun objet, y compris le TPA de l'hôte.

Les autorisations globales étendent les autorisations sur les objets de balise

Les autorisations globales, c'est-à-dire des autorisations qui sont attribuées sur l'objet racine, complètent les autorisations sur les objets de balise lorsque celles-ci sont trop restrictives. Les autorisations vCenter Server n'affectent pas les objets de balise.

Par exemple, supposons que vous attribuez le privilège **Supprimer une balise vSphere** à l'utilisateur Robin au niveau racine, en utilisant les autorisations globales. Pour la production de balises, vous n'attribuez pas le privilège **Supprimer une balise vSphere** à Robin. Dans ce cas, Robin dispose du privilège, même pour la production de balises car il a l'autorisation globale. Si vous ne modifiez pas l'autorisation globale, vous ne pouvez pas restreindre les privilèges.

Tableau 2-2. Les autorisations globales complètent les autorisations au niveau des balises

Autorisation globale	Autorisation au niveau des balises	Autorisation valable
Robin dispose des privilèges **Supprimer une balise vSphere**	Robin ne dispose pas des privilèges **Supprimer une balise vSphere** pour la balise.	Robin dispose des privilèges **Supprimer une balise vSphere**.
Aucun privilège de balisage accordé	Les privilèges **Supprimer une balise vSphere** ne sont pas attribués à Robin pour la balise.	Robin ne dispose pas des privilèges **Supprimer une balise vSphere**

Les autorisations au niveau des balises peuvent étendre les autorisations globales

Vous pouvez utiliser des autorisations au niveau des balises pour étendre les autorisations globales. Cela signifie que les utilisateurs peuvent avoir l'autorisation globale et l'autorisation au niveau des balises sur une balise.

Tableau 2-3. Les autorisations globales étendent les autorisations au niveau des balises

Autorisation globale	Autorisation au niveau des balises	Autorisation valable
Lee dispose du privilège **Attribuer une balise vSphere ou en annuler l'attribution**.	Lee dispose du privilège **Supprimer une balise vSphere**.	Lee dispose des privilèges **Attribuer une balise vSphere** et **Supprimer une balise vSphere** pour la balise.
Aucun privilège de balisage n'est accordé.	Le privilège **Supprimer une balise vSphere** est attribué à Lee pour la balise.	Lee dispose du privilège **Supprimer une balise vSphere** pour la balise.

Utilisation des rôles pour assigner des privilèges

Un rôle est un ensemble prédéfini de privilèges. Les privilèges définissent les droits permettant d'effectuer des actions et de lire des propriétés. Par exemple, le rôle Administrateur de machines virtuelles permet à un utilisateur de lire et de modifier les attributs de machines virtuelles.

Lorsque vous attribuez des autorisations, vous couplez un utilisateur ou un groupe avec un rôle et associez ce couplage à un objet d'inventaire. Un utilisateur ou groupe peut avoir différents rôles pour différents objets de l'inventaire.

Par exemple, supposez que votre inventaire comprend deux pools de ressources, le pool A et le pool B ; vous pouvez attribuer au groupe Ventes le rôle Utilisateur de machine virtuelle sur le pool A et le rôle Lecture seule sur le pool B. Ainsi, les utilisateurs du groupe Ventes peuvent démarrer les machines virtuelles du pool A, mais uniquement afficher les machines virtuelles du pool B.

vCenter Server fournit les rôles système et les exemples de rôles par défaut.

Rôles système Les rôles système sont permanents. Vous ne pouvez pas éditer les privilèges liés à ces rôles.

Exemples de rôles VMware fournit des exemples de rôles pour certaines combinaisons réalisées fréquemment. Vous pouvez cloner, modifier ou supprimer ces rôles.

Remarque Pour éviter de perdre les paramètres prédéfinis dans un exemple de rôle, clonez d'abord le rôle, puis modifiez le clone. Vous ne pouvez pas rétablir les paramètres par défaut de l'exemple.

Les utilisateurs ne peuvent planifier des tâches que si leurs rôles leur donnent des privilèges suffisants pour réaliser ces tâches au moment de leur création.

Remarque Les modifications apportées aux rôles et aux privilèges prennent effet immédiatement, même si les utilisateurs impliqués sont connectés. Les recherches font toutefois exception : pour celles-ci, les modifications entrent en vigueur une fois que l'utilisateur s'est déconnecté, puis reconnecté.

Rôles personnalisés dans vCenter Server et ESXi

Vous pouvez créer des rôles personnalisés pour vCenter Server et tous les objets qu'il gère, ou pour des hôtes individuels.

Rôles personnalisés de vCenter Server (recommandé) Créez des rôles personnalisés à l'aide des fonctionnalités de modification de rôles de vSphere Web Client afin de créer des ensembles de privilèges répondant spécifiquement à vos besoins.

Rôles personnalisés d'ESXi Vous pouvez créer des rôles personnalisés pour des hôtes individuels en utilisant une interface de ligne de commande ou VMware Host Client. Consultez la documentation de *Gestion individuelle des hôtes vSphere - VMware Host Client*. Les rôles d'hôtes personnalisés ne sont pas accessibles à partir de vCenter Server.

Si vous gérez des hôtes ESXi via vCenter Server, ne conservez pas de rôles personnalisés dans l'hôte et dans vCenter Server. Définissez les rôles au niveau de vCenter Server.

Lorsque vous gérez un hôte à l'aide de vCenter Server, les autorisations associées à cet hôte sont créées via vCenter Server et stockées dans vCenter Server. Si vous vous connectez directement à un hôte, seuls les rôles créés directement sur l'hôte sont disponibles.

Remarque Lorsque vous ajoutez un rôle personnalisé auquel vous n'attribuez aucun privilège, le rôle est créé comme un rôle Lecture seule avec trois privilèges définis par le système : **Système.Anonyme**, **Système.Affichage** et **Système.Lecture**.

Création de rôles dans vSphere Web Client (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_creating_role_in_vsphere_webclient)

Rôles système de vCenter Server

Un rôle est un ensemble prédéfini de privilèges. Lorsque vous ajoutez des autorisations à un objet, vous associez un utilisateur ou un groupe à un rôle. vCenter Server comprend plusieurs rôles système que vous ne pouvez pas modifier.

Rôles système de vCenter Server

vCenter Server fournit des rôles par défaut. Vous ne pouvez pas changer les privilèges associés aux rôles par défaut. Les rôles par défaut sont organisés de façon hiérarchique. Chaque rôle hérite des privilèges du rôle précédent. Par exemple, le rôle Administrateur hérite des privilèges du rôle Lecture seule. Les rôles que vous créez vous-même n'héritent des privilèges d'aucun rôle système.

Rôle d'administrateur

Les utilisateurs qui ont le rôle Administrateur pour un objet sont autorisés à afficher et à exécuter toutes les actions sur cet objet. Ce rôle comprend également tous les privilèges inhérents au rôle en lecture seule. Si vous disposez du rôle d'administrateur sur un objet, vous pouvez attribuer des privilèges à des utilisateurs individuels ou des groupes. Si vous disposez du rôle d'administrateur dans vCenter Server, vous pouvez attribuer des privilèges à des utilisateurs et des groupes dans la source d'identité vCenter Single Sign-On par défaut. Les services d'identité pris en charge incluent Windows Active Directory et OpenLDAP 2.4.

Par défaut, l'utilisateur administrator@vsphere.local a le rôle d'administrateur sur vCenter Single Sign-On et vCenter Server après l'installation. Cet utilisateur peut ensuite associer d'autres utilisateurs disposant du rôle d'administrateur dans vCenter Server.

Rôle Aucun administrateur de chiffrement

Les utilisateurs qui ont le rôle Aucun administrateur de chiffrement pour un objet ont les mêmes privilèges que les utilisateurs ayant le rôle Administrateur, à l'exception des privilèges pour les **opérations de chiffrement**. Ce rôle permet aux administrateurs de désigner d'autres administrateurs qui ne peuvent pas chiffrer ou déchiffrer des machines virtuelles ni accéder aux données chiffrées, mais qui peuvent effectuer les autres tâches d'administration.

rôle Aucun accès

Les utilisateurs qui ont le rôle Aucun accès pour un objet ne peuvent en aucun cas afficher ou modifier l'objet. Les nouveaux utilisateurs et groupes sont assignés à ce rôle par défaut. Vous pouvez modifier le rôle par objet.

Le rôle Administrateur est attribué par défaut à l'administrateur du domaine vCenter Single Sign-On (par défaut administrator@vsphere.local) ainsi qu'aux utilisateurs racine et vpxuser. Le rôle Aucun accès est attribué par défaut aux autres utilisateurs.

rôle Lecture seule

Les utilisateurs qui ont le rôle Lecture seule pour un objet sont autorisés à afficher l'état et les détails de l'objet. Par exemple, les utilisateurs ayant ce rôle peuvent afficher la machine virtuelle, l'hôte et les attributs du pool de ressources, mais ne peuvent pas afficher la console distante d'un hôte. Toutes les actions via les menus et barres d'outils ne sont pas autorisées.

La meilleure pratique consiste à créer un utilisateur au niveau racine et à lui attribuer le rôle Administrateur. Après avoir créé un utilisateur nommé ayant les privilèges Administrateur, vous ne pouvez pas supprimer l'utilisateur racine des autorisations ni remplacer son rôle par le rôle Aucun accès.

Créer un rôle personnalisé

Vous pouvez créer des rôles personnalisés vCenter Server correspondant aux besoins de contrôle d'accès de votre environnement.

Si vous créez ou modifiez un rôle sur un système vCenter Server qui fait partie du même domaine vCenter Single Sign-On que les autres systèmes vCenter Server, le service d'annuaire VMware (vmdir) propage les modifications que vous apportez à tous les autres systèmes vCenter Server du groupe. Cependant, les attributions de rôles à des utilisateurs et objets spécifiques ne sont pas partagées entre les systèmes vCenter Server.

Prérequis

Vérifiez que vous êtes connecté en tant qu'utilisateur avec des privilèges d'administrateur.

Procédure

1 Connectez-vous à vCenter Server avec vSphere Web Client.

2 Sélectionnez Accueil, cliquez sur **Administration**, puis cliquez sur **Rôles**.

3 Cliquez sur le bouton **Créer une action de rôle** (+).

4 Introduire un nom pour le nouveau rôle.

5 Sélectionner les privilèges pour le rôle et cliquer sur **OK**.

Cloner un rôle

Vous pouvez effectuer une copie d'un rôle existant, le renommer et le modifier. Quand vous faites une copie, le nouveau rôle n'est pas appliqué à n'importe quel utilisateur ou groupe et objet. Vous devez attribuer le rôle aux utilisateurs ou groupes et objets.

Si vous créez ou modifiez un rôle sur un système vCenter Server qui fait partie du même domaine vCenter Single Sign-On que les autres systèmes vCenter Server, le service d'annuaire VMware (vmdir) propage les modifications que vous apportez à tous les autres systèmes vCenter Server du groupe. Cependant, les attributions de rôles à des utilisateurs et objets spécifiques ne sont pas partagées entre les systèmes vCenter Server.

Prérequis

Vérifiez que vous êtes connecté en tant qu'utilisateur avec des privilèges d'administrateur.

Procédure

1 Connectez-vous à vCenter Server avec vSphere Web Client.

2 Sélectionnez Accueil, cliquez sur **Administration**, puis cliquez sur **Rôles**.

3 Sélectionnez un rôle et cliquez sur l'icône **Cloner une action de rôle**.

4 Saisissez un nom pour le rôle cloné.

5 Sélectionnez ou désélectionnez des privilèges pour le rôle, puis cliquez sur **OK**.

Éditer un rôle

Quand vous éditez un rôle, vous pouvez changer les privilèges sélectionnés pour ce rôle. Une fois terminés, ces privilèges sont appliqués à n'importe quel utilisateur ou groupe auquel le rôle modifié a été attribué.

Si vous créez ou modifiez un rôle sur un système vCenter Server qui fait partie du même domaine vCenter Single Sign-On que les autres systèmes vCenter Server, le service d'annuaire VMware (vmdir) propage les modifications que vous apportez à tous les autres systèmes vCenter Server du groupe. Cependant, les attributions de rôles à des utilisateurs et objets spécifiques ne sont pas partagées entre les systèmes vCenter Server.

Prérequis

Vérifiez que vous êtes connecté en tant qu'utilisateur avec des privilèges d'administrateur.

Procédure

1 Connectez-vous à vCenter Server avec vSphere Web Client.

2 Sélectionnez Accueil, cliquez sur **Administration**, puis cliquez sur **Rôles**.

3 Sélectionnez un rôle, puis cliquez sur le bouton **Modifier une action de rôle**.

4 Sélectionnez ou désélectionnez des privilèges pour le rôle, puis cliquez sur **OK**.

Meilleures pratiques pour les rôles et les autorisations

Utilisez les meilleures pratiques pour les rôles et les autorisations afin de maximiser la sécurité et la gérabilité de votre environnement vCenter Server.

VMware recommande les meilleures pratiques suivantes lorsque vous configurez les rôles et les autorisations dans votre environnement vCenter Server :

- Lorsque cela est possible, attribuez un rôle à un groupe plutôt qu'à des utilisateurs individuels pour accorder des privilèges à ce groupe.
- Accordez des autorisations uniquement sur les objets lorsque cela est nécessaire et attribuez des privilèges uniquement aux utilisateurs ou aux groupes qui doivent en disposer. Utiliser un nombre minimal d'autorisations facilite la compréhension et la gestion de votre structure d'autorisations.
- Si vous assignez un rôle restrictif à un groupe, vérifiez que le groupes ne contient pas l'utilisateur d'administrateur ou d'autres utilisateurs avec des privilèges administratifs. Sinon, vous pourriez involontairement limiter les privilèges des administrateurs dans les parties de la hiérarchie d'inventaire où vous avez assigné à ce groupes le rôle restrictif.
- Utilisez des dossiers pour grouper des objets. Par exemple, si vous souhaitez accorder une autorisation de modification sur un ensemble d'hôtes et afficher une autorisation sur un autre ensemble d'hôtes, placez chaque ensemble d'hôtes dans un dossier.
- Soyez prudent lorsque vous ajoutez une autorisation aux objets vCenter Server racine. Les utilisateurs disposant de privilèges au niveau racine ont accès à des données globales sur vCenter Server, telles que les rôles, les attributs personnalisés et les paramètres vCenter Server.
- Dans la plupart des cas, activez la propagation lorsque vous attribuez des autorisations à un objet. Ceci garantit que quand de nouveaux objets sont insérés dans la hiérarchie d'inventaire, ils héritent des autorisations et sont accessibles aux utilisateurs.
- Utilisez le rôle Aucun Accès pour masquer des zones spécifiques de la hiérarchie si vous souhaitez empêcher l'accès de certains utilisateurs ou groupes aux objets qui se trouvent dans cette partie de la hiérarchie d'objets.

- Les modifications apportées aux licences sont appliquées à tous les systèmes vCenter Server qui sont liés au même Platform Services Controller ou aux Platform Services Controller se trouvant dans le même domaine vCenter Single Sign-On, même si l'utilisateur ne dispose pas de privilèges sur tous les systèmes vCenter Server.

Privilèges requis pour les tâches courantes

Beaucoup de tâches exigent des autorisations sur plus d'un objet dans l'inventaire. Vous pouvez passer en revue les privilèges requis pour exécuter les tâches et, le cas échéant, les rôles modèles appropriés.

Le tableau suivant répertorie les tâches courantes qui exigent plusieurs privilèges. Vous pouvez ajouter des autorisations à des objets d'inventaire en associant un utilisateur à l'un des rôles prédéfinis. Vous pouvez également créer des rôles personnalisés avec l'ensemble des privilèges que vous prévoyez d'utiliser plusieurs fois.

Si la tâche que vous souhaitez exécuter ne se trouve pas dans ce tableau, les règles suivantes peuvent vous aider à déterminer l'emplacement dans lequel vous devez attribuer des autorisations pour autoriser certaines opérations :

- N'importe quelle opération qui consomme l'espace de stockage, telle que la création d'un disque virtuel ou la prise d'un snapshot, exige le privilège **Banque de données.Allouer l'espace** sur la banque de données cible, ainsi que le privilège d'exécuter l'opération elle-même.
- Le déplacement d'un objet dans la hiérarchie d'inventaire exige les privilèges appropriés sur l'objet lui-même, l'objet parent source (tel qu'un dossier ou un cluster) et l'objet parent de destination.
- Chaque hôte et chaque cluster ont leur propre pool de ressources implicite qui contient toutes les ressources de cet hôte ou de ce cluster. Le déploiement d'une machine virtuelle directement sur un hôte ou un cluster exige le privilège **Ressource.Attribuer une machine virtuelle au pool de ressources**.

Tableau 2-4. Privilèges requis pour les tâches courantes

Tâche	Privilèges requis	Rôle applicable
Créer une machine virtuelle	Dans le dossier ou le centre de données de destination : ■ **Machine virtuelle .Inventaire.Créer** ■ **Machine virtuelle.Configuration.Ajouter un nouveau disque** (en cas de création d'un nouveau disque virtuel) ■ **Machine virtuelle.Configuration.Ajouter un disque existant** (en cas d'utilisation d'un disque virtuel existant) ■ **Machine virtuelle.Configuration.Périphérique brut** (en cas d'utilisation d'un périphérique de relais RDM ou SCSI)	Administrateur
	Sur l'hôte, cluster ou pool de ressources de destination : **Ressource.Attribuer une machine virtuelle au pool de ressources**	Administrateur de pool de ressources ou Administrateur
	Sur la banque de données ou le dossier de destination contenant une banque de données : **Banque de données.Allouer de l'espace**	Utilisateur de banque de données ou Administrateur
	Sur le réseau auquel la machine virtuelle sera assignée : **Réseau.Attribuer un réseau**	Utilisateur réseau ou Administrateur
Déployer une machine virtuelle à partir d'un modèle	Dans le dossier ou le centre de données de destination : ■ **Machine virtuelle .Inventaire.Créer à partir d'un modèle existant** ■ **Machine virtuelle.Configuration.Ajouter un nouveau disque**	Administrateur
	Sur un modèle ou un dossier des modèles : **Machine virtuelle .Provisionnement.Déployer un modèle**	Administrateur

Tableau 2-4. Privilèges requis pour les tâches courantes (suite)

Tâche	Privilèges requis	Rôle applicable
	Sur l'hôte, le cluster ou le pool de ressources de destination : **Ressource.Attribuer une machine virtuelle au pool de ressources**	Administrateur
	Sur la banque de données de destination ou le dossier des banques de données : **Banque de données.Allouer de l'espace**	Utilisateur de banque de données ou Administrateur
	Sur le réseau auquel la machine virtuelle sera assignée : **Réseau.Attribuer un réseau**	Utilisateur réseau ou Administrateur
Faire un snapshot de machine virtuelle	Sur la machine virtuelle ou un dossier des machines virtuelles : **Machine virtuelle .Gestion des snapshots. Créer un snapshot**	Utilisateur avancé de machines virtuelles ou Administrateur
Déplacer une machine virtuelle dans un pool de ressources	Sur la machine virtuelle ou le dossier des machines virtuelles : ■ **Ressource.Attribuer une machine virtuelle au pool de ressources** ■ **Machine virtuelle .Inventaire.Déplacer**	Administrateur
	Sur le pool de ressources de destination : **Ressource.Attribuer une machine virtuelle au pool de ressources**	Administrateur
Installer un système d'exploitation invité sur une machine virtuelle	Sur la machine virtuelle ou le dossier des machines virtuelles : ■ **Machine virtuelle.Interaction .Répondre à une question** ■ **Machine virtuelle .Interaction .Interaction avec une console** ■ **Machine virtuelle .Interaction .Connexion à un périphérique** ■ **Machine virtuelle .Interaction .Mettre hors tension** ■ **Machine virtuelle .Interaction .Mettre sous tension** ■ **Machine virtuelle .Interaction .Réinitialiser** ■ **Machine virtuelle .Interaction .Configurer un support sur CD** (en cas d'installation à partir d'un CD) ■ **Machine virtuelle .Interaction .Configurer un support sur disquette** (en cas d'installation à partir d'une disquette) ■ **Machine virtuelle .Interaction .Installation de VMware Tools**	Utilisateur avancé de machines virtuelles ou Administrateur
	Sur une banque de données contenant l'image ISO de support d'installation : **Banque de données.Parcourir une banque de données** (en cas d'installation à partir d'une image ISO sur une banque de données) Sur la banque de données sur laquelle vous chargez l'image ISO de support d'installation : ■ **Banque de données.Parcourir une banque de données** ■ **Banque de données.Opérations de fichier de niveau inférieur**	Utilisateur avancé de machines virtuelles ou Administrateur
Migrer une machine virtuelle avec vMotion	Sur la machine virtuelle ou le dossier des machines virtuelles : ■ **Ressource.Migrer une machine virtuelle sous tension** ■ **Ressource.Attribuer une machine virtuelle au pool de ressources** (si la destination est un pool de ressources différent de la source)	Administrateur de pool de ressources ou Administrateur
	Sur l'hôte, le cluster ou le pool de ressources de destination (si différent de la source) : **Ressource.Attribuer une machine virtuelle au pool de ressources**	Administrateur de pool de ressources ou Administrateur

Tableau 2-4. Privilèges requis pour les tâches courantes (suite)

Tâche	Privilèges requis	Rôle applicable
Migrer à froid (relocaliser) une machine virtuelle	Sur la machine virtuelle ou le dossier des machines virtuelles : ■ **Ressource.Migrer une machine virtuelle hors tension** ■ **Ressource.Attribuer une machine virtuelle au pool de ressources** (si la destination est un pool de ressources différent de la source)	Administrateur de pool de ressources ou Administrateur
	Sur l'hôte, le cluster ou le pool de ressources de destination (si différent de la source) : **Ressource.Attribuer une machine virtuelle au pool de ressources**	Administrateur de pool de ressources ou Administrateur
	Sur la banque de données de destination (si différent de la source) : **Banque de données.Allouer de l'espace**	Utilisateur de banque de données ou Administrateur
Migration d'une machine virtuelle avec Storage vMotion	Sur la machine virtuelle ou le dossier des machines virtuelles : **Ressource.Migrer une machine virtuelle sous tension**	Administrateur de pool de ressources ou Administrateur
	Sur la banque de données de destination : **Banque de données.Allouer de l'espace**	Utilisateur de banque de données ou Administrateur
Déplacer un hôte dans un cluster	Sur l'hôte : **Hôte.Inventaire.Ajouter un hôte au cluster**	Administrateur
	Sur le cluster de destination : **Hôte.Inventaire.Ajouter un hôte au cluster**	Administrateur

Sécurisation des hôtes ESXi 3

L'architecture de l'hyperviseur ESXi intègre de nombreuses fonctionnalités de sécurité, telles que l'isolation du CPU, l'isolation de la mémoire et l'isolation des périphériques. Vous pouvez configure des fonctionnalités supplémentaires, comme le mode de verrouillage, le remplacement de certificats et l'authentification par carte à puce, pour renforcer la sécurité.

Un hôte ESXi est également protégé par un pare-feu. Vous pouvez ouvrir les ports au trafic entrant et sortant selon vos besoins, mais limitez l'accès aux services et aux ports. L'utilisation du mode verrouillage ESXi et la limitation de l'accès à ESXi Shell peuvent également contribuer à sécuriser davantage l'environnement. À partir de vSphere 6.0, les hôtes ESXi participent à l'infrastructure de certificats. Les hôtes sont provisionnés à l'aide de certificats signés par l'autorité de certification VMware (VMCA) par défaut.

Pour plus d'informations sur la sécurité d'*ESXi*, reportez-vous au livre blanc VMware ESXi.

Ce chapitre aborde les rubriques suivantes :

Configurer des hôtes ESXi avec des profils d'hôte

Les profils d'hôte vous permettent de définir des configurations standard pour vos hôtes ESXi et d'automatiser la conformité avec ces paramètres de configuration. Les profils d'hôte permettent de contrôler de nombreux aspects de la configuration de l'hôte, notamment la mémoire, le stockage, la mise en réseau, etc.

Il est possible de configurer les profils d'hôte d'un hôte de référence à partir de vSphere Web Client et d'appliquer un profil d'hôte à tous les hôtes partageant les caractéristiques de l'hôte de référence. Vous pouvez également utiliser les profils d'hôte pour surveiller les hôtes à la recherche de modifications de la configuration des hôtes. Consultez la documentation de *Profils d'hôte vSphere*.

Vous pouvez associer le profil d'hôte à un cluster afin de l'appliquer à tous ses hôtes.

Procédure

1 Configurez l'hôte de référence conformément aux spécifications et créez le profil d'hôte.

2 Associez le profil à un hôte ou à un cluster.

3 Appliquez le profil d'hôte de l'hôte de référence à tous les autres hôtes ou clusters.

Recommandations générales de sécurité pour ESXi

Pour protéger un hôte ESXi contre les intrusions et autorisations illégales, VMware impose des contraintes au niveau de plusieurs paramètres et activités. Vous pouvez atténuer les contraintes pour répondre à vos besoins de configuration. Dans ce cas, assurez-vous de travailler dans un environnement de confiance et prenez d'autres mesures de sécurité.

Fonctionnalités de sécurité intégrées

Les risques encourus par les hôtes sont limités par défaut, de la façon suivante :

- ESXi Shell et SSH sont désactivés par défaut.
- Un nombre limité de ports de pare-feu sont ouverts par défaut. Vous pouvez ouvrir explicitement des ports de pare-feu supplémentaires associés à des services spécifiques.
- ESXi exécute uniquement les services essentiels pour gérer ses fonctions. La distribution est limitée aux fonctionnalités requises pour exécuter ESXi.
- Par défaut, tous les ports non requis pour l'accès de gestion à l'hôte sont fermés. Ouvrez les ports si vous avez besoin de services supplémentaires.
- Par défaut, les chiffrements faibles sont désactivés et les communications provenant des clients sont sécurisées par SSL. Les algorithmes exacts utilisés pour la sécurisation du canal dépendant de l'algorithme de négociation SSL. Les certificats par défaut créés sur ESXi utilisent PKCS#1 SHA-256 avec le chiffrement RSA comme algorithme de signature.
- Un service Web Tomcat est utilisé en interne par ESXi pour prendre en charge l'accès par les clients Web. Le service a été modifié pour exécuter uniquement les fonctions dont un client Web a besoin pour l'administration et la surveillance. Par conséquent, ESXi n'est pas vulnérable aux problèmes de sécurité Tomcat signalés lors d'utilisations massives.
- VMware assure la surveillance de toutes les alertes de sécurité susceptibles d'affecter la sécurité d'ESXi et envoie un correctif de sécurité en cas de besoin.
- Les services non sécurisés (tels que FTP et Telnet) ne sont pas installés, et les ports associés à ces services sont fermés par défaut. Vous trouverez facilement des services plus sécurisés tels que SSH et SFTP. Il est donc conseillé de les privilégier et d'éviter d'utiliser les services non sécurisés. Par exemple, utilisez Telnet avec SSL pour accéder aux ports série virtuels si SSH n'est pas disponible et que vous devez utiliser Telnet.

  Si vous devez utiliser des services non sécurisés et que l'hôte bénéficie d'un niveau suffisant de sécurité, vous pouvez ouvrir des ports explicitement pour les prendre en charge.
- Envisagez d'utiliser le démarrage sécurisé UEFI pour votre système ESXi. Reportez-vous à « Démarrage sécurisé UEFI des hôtes ESXi », page 101.

Mesures de sécurité supplémentaires

Tenez compte des recommandations suivantes lorsque vous évaluez la sécurité de l'hôte et l'administration.

Limiter l'accès

Si vous activez l'accès à l'interface DCUI (Direct Console User Interface), ESXi Shell ou SSH impose des stratégies de sécurité d'accès strictes.

L'ESXi Shell possède un accès privilégié à certaines parties de l'hôte. Octroyez un accès de connexion à ESXi Shell uniquement aux utilisateurs approuvés.

Ne pas accéder directement aux hôtes gérés

Utilisez vSphere Web Client pour administrer les hôtes ESXi qui sont gérés par vCenter Server. N'accédez pas aux hôtes gérés directement avec VMware Host Client et ne modifiez pas les hôtes gérés à partir de l'interface DCUI.

Si vous gérez les hôtes à l'aide d'une interface de script ou d'une API, ne ciblez pas directement l'hôte. Ciblez plutôt le système vCenter Server qui gère l'hôte et spécifiez le nom de l'hôte.

Utiliser l'interface DCUI pour le dépannage

Accédez à l'hôte via l'interface DCUI ou ESXi Shell en tant qu'utilisateur racine uniquement pour le dépannage. Pour administrer vos hôtes ESXi, utilisez un des clients d'interface utilisateur ou une des API ou des interfaces de ligne de commande VMware. Si vous utilisez ESXi Shell ou SSH, limitez les comptes qui disposent d'un accès et définissez des délais d'expiration.

N'utilisez que des sources VMware pour mettre à niveau les composants ESXi.

L'hôte exécute plusieurs modules tiers pour prendre en charge les interfaces de gestion ou les tâches que vous devez effectuer. VMware prend en charge uniquement les mises à niveau vers les modules provenant d'une source VMware. Si vous utilisez un téléchargement ou un correctif provenant d'une autre source, cela risque de porter préjudice à la sécurité ou aux fonctions de l'interface de gestion. Consultez les sites Web des fournisseurs tiers et la base de connaissances VMware pour connaître les alertes de sécurité.

Remarque Suivez les instructions de sécurité fournies par VMware, disponible sur le site http://www.vmware.com/security/.

Utiliser des scripts pour gérer des paramètres de configuration d'hôte

Dans les environnements comportant de nombreux hôtes, la gestion des hôtes avec des scripts est plus rapide et moins susceptible de provoquer des erreurs que la gestion des hôtes depuis vSphere Web Client.

vSphere inclut plusieurs langages de script pour la gestion des hôtes. Reportez-vous à la *Documentation sur la ligne de commande de vSphere* et à la *Documentation sur vSphere API/SDK* pour obtenir des informations de référence et des astuces de programmation, et pour accéder à des communautés VMware afin d'obtenir des conseils supplémentaires sur la gestion par scripts. La documentation de l'administrateur de vSphere est principalement axée sur l'utilisation de vSphere Web Client pour la gestion.

vSphere PowerCLI

VMware vSphere PowerCLI est une interface Windows PowerShell avec vSphere API. Elle inclut des applets de commande PowerShell pour l'administration des composants vSphere.

	vSphere PowerCLI inclut plus de 200 applets de commande, un ensemble d'exemples de scripts et une bibliothèque de fonctions pour la gestion et l'automatisation. Reportez-vous à la *Documentation de vSphere PowerCLI*.
vSphere Command-Line Interface (vCLI)	vCLI inclut un ensemble de commandes pour la gestion des hôtes ESXi et des machines virtuelles. Le programme d'installation, qui installe également le vSphere SDK for Perl, s'exécute sur les systèmes Windows ou Linux, et installe des commandes ESXCLI, des commandes vicfg- et un ensemble d'autres commandes vCLI. Reportez-vous à la *Documentation de vSphere Command-Line Interface*.

À partir de vSphere 6.0, vous pouvez également utiliser l'une des interfaces de script au vCloud Suite SDK, comme vCloud Suite SDK for Python.

Procédure

1 Créez un rôle personnalisé ayant des privilèges limités.

Par exemple, considérez la création d'un rôle disposant d'un ensemble de privilèges pour la gestion d'hôtes mais sans privilège pour la gestion de machines virtuelles, du stockage ou de la mise en réseau. Si le script que vous souhaitez utiliser extrait uniquement des informations, vous pouvez créer un rôle disposant de privilèges de lecture seule pour l'hôte.

2 Dans vSphere Web Client, créez un compte de service et attribuez-lui le rôle personnalisé.

Vous pouvez créer plusieurs rôles personnalisés avec différents niveaux d'accès si vous souhaitez que l'accès à certains hôtes soit assez limité.

3 Écrivez des scripts pour effectuer la vérification ou la modification de paramètres, puis exécutez-les.

Par exemple, vous pouvez vérifier ou définir le délai d'expiration interactif du shell d'un hôte de la façon suivante :

Langue	Commandes
vCLI (ESXCLI)	`esxcli <conn_options> system settings advanced get /UserVars/ESXiShellTimeOut` `esxcli --formatter=csv --format-param=fields="Path,Int Value" system settings advanced list | grep /UserVars/ESXiShellTimeOut`

PowerCLI	`#List UserVars.ESXiShellInteractiveTimeOut for each host Get-VMHost | Select Name, @{N="UserVars.ESXiShellInteractiveTimeOut";E={$_ | Get-AdvancedSetting -Name UserVars.ESXiShellInteractiveTimeOut | Select -ExpandProperty Value}}`
	
	`# Set UserVars.ESXiShellTimeOut to 900 on all hosts Get-VMHost | Foreach { Get-AdvancedSetting -Entity $_ -Name UserVars.ESXiShellInteractiveTimeOut | Set-AdvancedSetting -Value 900 }`

4 Dans les environnements de grande envergure, créez des rôles avec des privilèges d'accès différents et des hôtes du groupe dans des dossiers en fonction des tâches que vous souhaitez effectuer. Vous pouvez ensuite exécuter des scripts sur les différents dossier depuis les différents comptes de service.

5 Vérifiez que les modifications ont été appliquées après l'exécution de la commande.

Verrouillage des mots de passe et des comptes ESXi

Pour les hôtes ESXi, vous devez utiliser un mot de passe avec des exigences prédéfinies. Vous pouvez modifier la longueur requise et l'exigence de classes de caractères ou autoriser les phrases secrètes à l'aide de l'option avancée `Security.PasswordQualityControl`.

ESXi utilise le module Linux PAM `pam_passwdqc` pour la gestion et le contrôle des mots de passe. Pour plus d'informations, reportez-vous aux pages du manuel concernant `pam_passwdqc`.

Remarque Les exigences par défaut pour les mots de passe ESXi dépendent de la version. Vous pouvez vérifier et modifier les restrictions de mot de passe par défaut à l'aide de l'option avancée `Security.PasswordQualityControl`.

Mots de passe d' ESXi

ESXi exige un mot de passe pour un accès à partir de l'interface DCUI (Direct Console User Interface), d'ESXi Shell, de SSH ou de VMware Host Client. Lorsque vous créez un mot de passe, vous devez inclure par défaut un mélange de quatre classes de caractères : lettres en minuscule, lettres en majuscule, chiffres et caractères spéciaux comme un trait de soulignement ou un tiret.

Remarque Un caractère en majuscule au début d'un mot de passe ne compte pas dans le nombre de classes de caractères utilisées. Un chiffre à la fin d'un mot de passe ne compte pas dans le nombre de classes de caractères utilisées.

Les mots de passe ne doivent pas contenir un mot du dictionnaire ou une partie d'un mot du dictionnaire.

Exemple de mots de passe d' ESXi

Les candidats de mot de passe suivants illustrent les mots de passe possibles si l'option est définie de la manière suivante.

```
retry=3 min=disabled,disabled,disabled,7,7
```

Avec ce paramètre, les mots de passe avec une ou deux classes de caractères et les phrases secrètes ne sont pas autorisés, car les trois premiers éléments sont désactivés. Les mots de passe composés de trois et quatre classes de caractères exigent sept caractères. Pour plus d'informations, reportez-vous à page du manuel concernant `pam_passwdqc`.

Avec ces paramètres, les mots de passe suivants sont autorisés.

- xQaTEhb!: contient huit caractères provenant de trois classes de caractères.
- xQaT3#A : contient sept caractères provenant de quatre classes de caractères.

Les candidats de mot de passe suivants ne répondent pas aux exigences.

- Xqat3hi : commence par un caractère majuscule, réduisant ainsi le nombre effectif de classes de caractères à deux. Trois classes de caractères au minimum sont exigées.
- xQaTEh2 : se termine par un chiffre, réduisant ainsi le nombre effectif de classes de caractères à deux. Trois classes de caractères au minimum sont exigées.

Phrase secrète ESXi

Vous pouvez également utiliser une phrase secrète à la place d'un mot de passe. Néanmoins, les phrases secrètes sont désactivées par défaut. Vous pouvez modifier cette valeur par défaut ou d'autres paramètres à l'aide de `Security.PasswordQualityControl` l'option avancée depuis vSphere Web Client.

Par exemple, vous pouvez remplacer l'option par la suivante.

```
retry=3 min=disabled,disabled,16,7,7
```

Cet exemple autorise des phrases secrètes d'au moins 16 caractères et d'au moins 3 mots, séparés par des espaces.

Pour les hôtes hérités, la modification du fichier `/etc/pamd/passwd` est toujours autorisée, mais vous ne pourrez plus le modifier dans les futures versions. Utilisez plutôt l'option avancée `Security.PasswordQualityControl`.

Modification des restrictions de mot de passe par défaut

Vous pouvez modifier les restrictions par défaut des mots de passe ou des phrases secrètes en utilisant l'option avancée `Security.PasswordQualityControl` de votre hôte ESXi. Reportez-vous à la documentation *Gestion de vCenter Server et des hôtes* pour obtenir plus d'informations sur la configuration des options avancées d'ESXi.

Vous pouvez modifier la valeur par défaut, par exemple, pour exiger un minimum de 15 caractères et un nombre minimal de quatre mots, comme suit :

```
retry=3 min=disabled,disabled,15,7,7 passphrase=4
```

Pour plus d'informations, reportez-vous à la page du manuel concernant `pam_passwdqc`.

Remarque Les combinaisons possibles des options de `pam_passwdqc` n'ont pas toutes été testées. Effectuez des tests supplémentaires après avoir modifié les paramètres du mot de passe par défaut.

Comportement de verrouillage de compte d' ESXi

À partir de vSphere 6.0, le verrouillage des comptes est pris en charge pour l'accès via SSH et vSphere Web Services SDK. L'interface de console directe (DCUI) et ESXi Shell ne prennent pas en charge le verrouillage de compte. Par défaut, un nombre maximal de dix tentatives de connexion échouées est autorisé avant le verrouillage du compte. Par défaut, le compte est déverrouillé au bout de deux minutes.

Configuration du comportement de connexion

Vous pouvez configurer le comportement de connexion de votre hôte ESXi à l'aide des options avancées suivantes :

- `Security.AccountLockFailures`. Nombre maximal de tentatives de connexion échouées autorisées avant le verrouillage du compte de l'utilisateur. La valeur zéro désactive le verrouillage du compte.
- `Security.AccountUnlockTime`. Nombre de secondes pendant lequel le compte d'un utilisateur est verrouillé.

Reportez-vous à la documentation *Gestion de vCenter Server et des hôtes* pour obtenir plus d'informations sur la configuration des options avancées d'ESXi.

Sécurité SSH

Vous pouvez utiliser SSH pour vous connecter à distance au ESXi Shell et accomplir des tâches de dépannage pour l'hôte.

La configuration SSH d'ESXi est améliorée et offre un haut niveau de sécurité.

Désactivation de la version 1 du protocole SSH	VMware ne prend pas en charge la version 1 du protocole SSH . Il utilise désormais exclusivement la version 2. La version 2 permet d'éliminer certains problèmes de sécurité qui se produisaient dans la version 1 et offre une communication plus sûre grâce à l'interface de gestion.
Chiffrement renforcé	Pour les connexions, SSH ne prend en charge que les chiffrements AES 256 bits et 128 bits.

Ces paramètres sont destinés à assurer une protection renforcée des données transmises à l'interface de gestion via SSH. Vous ne pouvez pas modifier ces paramètres.

Clés SSH ESXi

Vous pouvez utiliser des clés SSH pour restreindre, contrôler et sécuriser l'accès à un hôte ESXi. En utilisant une clé SSH, vous pouvez permettre à des utilisateurs ou des scripts approuvés de se connecter à un hôte sans spécifier le mot de passe.

Vous pouvez copier la clé SSH sur l'hôte en utilisant la commande `vifs` de l'interface de ligne de commande vSphere. Pour obtenir des informations sur l'installation et l'utilisation de l'ensemble de commandes de l'interface de ligne de commande vSphere, reportez-vous à *Démarrage avec les interfaces de ligne de commande vSphere*. Il est également possible d'utiliser HTTPS PUT pour copier la clé SSK sur l'hôte.

Au lieu de générer les clés en externe et de les télécharger, vous pouvez les créer sur l'hôte ESXi et les télécharger. Reportez-vous à l'article 1002866 de la base de connaissances VMware.

Activer SSH et ajouter des clés SSH à l'hôte présente des risques inhérents. Évaluez le risque potentiel d'exposer un nom d'utilisateur et un mot de passe par rapport au risque d'intrusion par un utilisateur qui dispose d'une clé approuvée.

Remarque Dans ESXi 5.0 et versions ultérieures, un utilisateur disposant d'une clé SSH peut accéder à l'hôte même lorsque ce dernier est en mode verrouillage. À partir de ESXi 5.1, un utilisateur ayant une clé SSH ne peut plus accéder à un hôte qui est en mode de verrouillage.

Charger une clé SSH à l'aide d'une commande vifs

Si vous décidez d'utiliser des clés autorisées pour vous connecter à un hôte avec SSH, vous pouvez télécharger des clés autorisées avec une commande `vifs`.

Remarque Du fait que les clés autorisées permettent l'accès SSH sans nécessiter l'authentification de l'utilisateur, demandez-vous vraiment si vous voulez utiliser des clés SSH dans votre environnement.

Les clés autorisées vous permettent d'authentifier un accès distant à un hôte. Lorsque des utilisateurs ou des scripts essaient d'accéder à un hôte avec SSH, la clé fournit l'authentification sans mot de passe. Les clés autorisées vous permettent d'automatiser l'authentification, ce qui est utile lorsque vous écrivez des scripts pour réaliser des tâches routinières.

Vous pouvez télécharger les types de clés SSH suivants sur un hôte.

- Fichier de clés autorisées pour un utilisateur racine
- Clé RSA
- Clé RSA publique

À partir de vSphere 6.0 Update 2, les clés DSS/DSA ne sont plus prises en charge.

Important Ne modifiez pas le fichier `/etc/ssh/sshd_config`.

Procédure

- Sur la ligne de commande ou un serveur d'administration, utilisez la commande `vifs` pour télécharger la clé SSH dans l'emplacement approprié sur l'hôte ESXi.

  ```
  vifs --server hostname --username username --put filename /host/ssh_host_dsa_key_pub
  ```

Type de clés :	Emplacement
Fichiers de clés autorisées pour un utilisateur racine	`/host/ssh_root_authorized keys` Vous devez bénéficier de tous les privilèges Administrateur pour télécharger ce fichier.
Clés RSA	`/host/ssh_host_rsa_key`
Clés RSA publiques	`/host/ssh_host_rsa_key_pub`

Charger une clé SSH à l'aide de HTTPS PUT

Vous pouvez utiliser des clés autorisées pour ouvrir une session sur un hôte avec SSH. Vous pouvez charger les clés autorisées à l'aide de HTTPS PUT.

Les clés autorisées vous permettent d'authentifier un accès distant à un hôte. Lorsque des utilisateurs ou des scripts essaient d'accéder à un hôte avec SSH, la clé fournit l'authentification sans mot de passe. Les clés autorisées vous permettent d'automatiser l'authentification, ce qui est utile lorsque vous écrivez des scripts pour réaliser des tâches routinières.

Vous pouvez télécharger les types de clés SSH suivants sur un hôte à l'aide de HTTPS PUT :

- Fichier de clés autorisées pour un utilisateur racine
- Clé DSA
- Clé DSA publique
- Clé RSA
- Clé RSA publique

Important Ne modifiez pas le fichier `/etc/ssh/sshd_config`.

Procédure

1 Dans votre application de chargement, ouvrez le fichier de clé.

2 Publiez le fichier aux emplacements suivants.

Type de clés :	Emplacement
Fichiers de clés autorisées pour un utilisateur racine	`https://hostname_or_IP_address/host/ssh_root_authorized_keys` Vous devez disposer de tous les privilèges Administrateur sur l'hôte pour télécharger ce fichier.
Clés DSA	`https://hostname_or_IP_address/host/ssh_host_dsa_key`
Clés DSA publiques	`https://hostname_or_IP_address/host/ssh_host_dsa_key_pub`
Clés RSA	`https://hostname_or_IP_address/host/ssh_host_rsa_key`
Clés RSA publiques	`https://hostname_or_IP_address/host/ssh_host_rsa_key_pub`

Périphériques PCI et PCIe et ESXi

L'utilisation de la fonctionnalité de VMware DirectPath I/O pour relayer un périphérique PCI ou PCIe vers une machine virtuelle crée une vulnérabilité de sécurité potentielle. La vulnérabilité peut être déclenchée par un code bogué ou malveillant tel qu'un pilote de périphérique qui s'exécuterait en mode privilégié dans le système d'exploitation invité. Le matériel et les microprogrammes standard actuels n'assurent pas un niveau suffisant de confinement des erreurs suffisant pour permettre à ESXi d'entièrement neutraliser la vulnérabilité.

VMware recommande d'utiliser un relais PCI ou PCIe vers une machine virtuelle uniquement si la machine virtuelle est détenue et administrée par une entité approuvée. Vous devez vous assurer que cette entité ne tente pas de bloquer ou d'exploiter l'hôte depuis la machine virtuelle.

Votre hôte peut être compromis de l'une des manières suivantes.

- Le système d'exploitation invité peut générer une erreur PCI ou PCIe irrécupérable. Une telle erreur n'altère pas les données, mais peut bloquer l'hôte ESXi. De telles erreurs peuvent se produire en raison de bogues et d'incompatibilités dans les périphériques matériels qui sont relayés, ou en raison de problèmes de pilotes du système d'exploitation invité.
- Le système d'exploitation invité peut générer une opération DMA (Direct Memory Access) qui provoque une erreur de page IOMMU sur l'hôte ESXi, par exemple, si l'opération DMA cible une adresse située hors de la mémoire de la machine virtuelle. Sur certaines machines, le microprogramme de l'hôte configure les fautes IOMMU pour signaler une erreur irrémédiable via une interruption non-masquable (NMI), ce qui entraîne le blocage de l'hôte ESXi. Ce problème peut être dû à des dysfonctionnements de pilotes du système d'exploitation invité.
- Si le système d'exploitation sur l'hôte ESXi n'utilise pas le remappage d'interruption, le système d'exploitation invité peut injecter une interruption fallacieuse dans l'hôte ESXi sur n'importe quel vecteur. ESXi utilise actuellement le remappage d'interruptions sur les plates-formes Intel offrant cette possibilité ; le remappage d'interruption fait partie de l'ensemble de fonctionnalités Intel VT-d. ESXi n'utilise pas le mappage d'interruptions sur les plates-formes AMD. Une interruption fallacieuse est susceptible de provoquer le blocage de l'hôte ESXi ; cependant, il peut théoriquement exister d'autres manières d'exploiter ces interruptions.

Désactiver Managed Object Browser

Le navigateur d'objets gérés (Managed Object Browser, MOB) permet d'explorer le modèle d'objet VMkernel. Cependant, les pirates peuvent utiliser cette interface pour effectuer des actions ou des modifications de configuration malveillantes, car il est possible de modifier la configuration de l'hôte à l'aide du MOB. Utilisez le MOB uniquement à des fins de débogage et assurez-vous qu'il est désactivé dans les systèmes de production.

À partir de vSphere 6.0, le MOB est désactivé par défaut. Cependant, pour certaines tâches, par exemple lors de l'extraction de l'ancien certificat d'un système, vous devez utiliser le MOB. Vous pouvez activer ou désactiver le MOB de la manière suivante.

Procédure

1 Sélectionnez l'hôte de vSphere Web Client, puis accédez à l'option **Paramètres système avancés**.

2 Contrôlez la valeur de **Config.HostAgent.plugins.solo.enableMob** et modifiez-la, le cas échéant.

N'utilisez pas la commande `vim-cmd` depuis ESXi Shell.

Recommandations de sécurité pour la mise en réseau d'ESXi

L'isolation du trafic réseau est essentielle pour un environnement ESXi sécurisé. Des réseaux différents requièrent un accès et un niveau d'isolation distincts.

Votre hôte ESXi utilise plusieurs réseaux. Utilisez des mesures de sécurité appropriées à chaque réseau et isolez le trafic pour des applications et fonctions spécifiques. Par exemple, assurez-vous que le trafic VMware vSphere vMotion® n'est pas acheminé via des réseaux sur lesquels se trouvent les machines virtuelles. L'isolation empêche l'écoute. Il est également recommandé d'utiliser des réseaux séparés pour des raisons de performance.

- Les réseaux de l'infrastructure vSphere sont utilisés pour certaines fonctions comme vSphere vMotion, VMware vSphere Fault Tolerance et le stockage. Isolez ces réseaux pour leurs fonctions spécifiques. Il n'est souvent pas nécessaire de router ces réseaux à l'extérieur d'un rack de serveur physique spécifique.
- Un réseau de gestion isole le trafic client, le trafic de l'interface de ligne de commande ou de l'API ou le trafic des logiciels tiers de tout autre trafic. Ce réseau doit être accessible uniquement aux administrateurs système, réseau et sécurité. Utilisez les systèmes JumpBox ou le réseau privé virtuel (VPN) pour sécuriser l'accès au réseau de gestion. Contrôlez strictement l'accès à ce réseau.
- Le trafic des machines virtuelles peut traverser un ou plusieurs réseaux. Vous pouvez renforcer l'isolation des machines virtuelles en utilisant des solutions de pare-feu qui définissent des règles de pare-feu au niveau du contrôleur du réseau virtuel. Ces paramètres sont acheminés avec une machine virtuelle dès lors qu'elle migre d'un hôte à un autre dans votre environnement vSphere.

Modifier les paramètres proxy Web ESXi

Lorsque vous modifiez les paramètres proxy Web, vous devez prendre en compte plusieurs recommandations de sécurité utilisateur et de chiffrement.

Remarque Redémarrez le processus hôte après avoir modifié les répertoires hôtes ou les mécanismes d'authentification.

- Ne configurez aucun certificat utilisant un mot de passe ou une phrase secrète. ESXi ne prend pas en charge les proxies Web qui utilisent des mots de passe ou des phrases secrètes (également appelés « clés chiffrées »). Si vous configurez un proxy Web qui nécessite un mot de passe ou une phrase secrète, les processus ESXi ne peuvent pas démarrer correctement.
- Pour assurer la prise en charge du chiffrement des noms d'utilisateur, des mots de passe et des paquets, SSL est activé par défaut pour les connexions vSphere Web Services SDK. Si vous souhaitez configurer ces connexions afin qu'elles ne chiffrent pas les transmissions, désactivez SSL pour votre connexion vSphere Web Services SDK en remplaçant le paramètre de connexion HTTPS par HTTP.

  Envisagez de mettre hors tension SSL uniquement si vous avez créé un environnement parfaitement fiable pour ces clients, avec des pare-feu et des transmissions depuis/vers l'hôte totalement isolées. La désactivation de SSL peut améliorer les performances car vous évitez le traitement requis pour l'exécution du chiffrement.
- Pour vous protéger contre les utilisations abusives des services ESXi, la plupart des services ESXi internes sont uniquement accessibles via le port 443, qui est utilisé pour la transmission HTTPS. Le port 443 agit comme proxy inversé pour ESXi. Vous pouvez consulter la liste de services sur ESXi via une page d'accueil HTTP, mais vous ne pouvez pas directement accéder aux services d'Adaptateurs de stockage sans autorisation.

  Vous pouvez modifier cette configuration afin que des services individuels soient directement accessibles via des connexions HTTP. N'effectuez pas ce changement à moins d'utiliser ESXi dans un environnement parfaitement fiable.
- Lorsque vous mettez votre environnement à niveau, le certificat est conservé.

Considérations relatives à la sécurité dans vSphere Auto Deploy

Lorsque vous utilisez vSphere Auto Deploy, soyez très vigilants à la sécurité du réseau, la sécurité de l'image de démarrage et l'éventuelle exposition des mots de passe dans les profils d'hôtes afin de protéger votre environnement.

Sécurité de la mise en réseau

Sécurisez votre réseau exactement comme si vous sécurisiez le réseau pour n'importe quelle autre méthode déploiement basée sur PXE. vSphere Auto Deploy transfère les données sur SSL pour éviter les interférences et les risques d'écoute. Toutefois, l'authenticité du client ou du serveur Auto Deploy n'est pas vérifiée au cours d'un démarrage PXE.

Vous pouvez considérablement réduire le risque de sécurité d'Auto Deploy en isolant complètement le réseau lorsqu'Auto Deploy est utilisé.

Sécurité concernant l'image de démarrage et le profil d'hôte

L'image de démarrage que le serveur vSphere Auto Deploy télécharge sur une machine peut contenir les composants suivants.

- Les modules VIB qui constituent le profil d'image sont toujours inclus dans l'image de démarrage.
- Le profil d'hôte et la personnalisation de l'hôte sont inclus dans l'image de démarrage si les règles Auto Deploy sont configurées pour provisionner l'hôte avec un profil d'hôte ou une personnalisation d'hôte.
  - Le mot de passe administrateur (racine) et les mots de passe utilisateur qui sont inclus dans le profil d'hôte et la personnalisation d'hôte sont cryptés en MD5.
  - Tous les autres mots de passe associés aux profils sont en clair. Si vous paramétrez Active Directory en utilisant des profils d'hôte, les mots de passe ne sont pas protégés.

    Utilisez vSphere Authentication Proxy afin d'éviter d'exposer les mots de passe d'Active Directory. Si vous paramétrez Active Directory en utilisant des profils d'hôte, les mots de passe sont protégés.
- La clé SSL publique et privée et le certificat de l'hôte sont inclus dans l'image de démarrage.

Contrôler l'accès aux outils de surveillance du matériel basée sur CIM

Le système CIM (Modèle de données unifié, Common Information Model) fournit une interface permettant la gestion au niveau du matériel à partir d'applications distantes utilisant un ensemble d'API standard. Pour garantir que l'interface CIM est sécurisée, ne fournissez que le niveau d'accès minimal nécessaire à ces applications distantes. Si vous provisionnez une application distante avec un compte racine ou d'administrateur, et si l'application est compromise, l'environnement virtuel peut l'être également.

Le modèle CIM est une norme ouverte qui définit une architecture pour la surveillance des ressources matérielles sans agent et basée sur des normes pour les hôtes ESXi. Cette structure se compose d'un gestionnaire d'objet CIM, généralement appelé courtier CIM, et d'un ensemble de fournisseurs CIM.

Les fournisseurs CIM prennent en charge l'accès de gestion aux pilotes des périphériques et au matériel sous-jacent. Les fournisseurs de matériel, y compris les fabricants de serveurs et les fournisseurs de périphériques matériel, peuvent inscrire les fournisseurs qui surveillent et gèrent leurs périphériques. VMware inscrit les fournisseurs qui surveillent le matériel de serveur, l'infrastructure de stockage ESXi et les ressources spécifiques à la virtualisation. Ces fournisseurs sont exécutés au sein de l'hôte ESXi. Ils sont légers et axés sur des tâches de gestion spécifiques. Le courtier CIM recueille les informations de tous les fournisseurs CIM et les présente à l'extérieur à l'aide d'API standard. L'API la plus standard est WS-MAN.

Ne fournissez pas aux applications distantes des informations d'identification racine permettant d'accéder à l'interface CIM. Créez plutôt un compte de service pour ces applications. Accordez un accès en lecture seule aux informations CIM à tous les comptes locaux définis sur le système ESXi, ainsi qu'à tous les rôles définis dans vCenter Server.

Procédure

1 Créez un compte de service pour les applications CIM.

2 Accordez un accès en lecture seule de compte de service aux hôtes ESXi qui collectent les informations CIM.

3 (Facultatif) Si l'application requiert un accès en écriture, créez un rôle avec deux privilèges seulement.

- **Hôte.Config.SystemManagement (Gestion du système)**
- **Hôte.CIM.CIMInteraction (Interaction CIM)**

4 Pour chaque hôte ESXi que vous surveillez, créez une autorisation qui couple le rôle personnalisé avec le compte de service.

Reportez-vous à « Utilisation des rôles pour assigner des privilèges », page 32.

Gestion de certificats pour les hôtes ESXi

Dans vSphere 6.0 et versions ultérieures, VMware Certificate Authority (VMCA) provisionne chaque nouvel hôte ESXi avec un certificat signé dont VMCA est l'autorité de certification racine par défaut. Le provisionnement s'effectue lorsque l'hôte est explicitement ajouté à vCenter Server ou dans le cadre d'une installation ou d'une mise à niveau vers ESXi 6.0 ou version ultérieure.

Vous pouvez afficher et gérer les certificats ESXi depuis vSphere Web Client et en utilisant l'API `vim.CertificateManager` dans vSphere Web Services SDK. Vous ne pouvez pas afficher ou gérer des certificats ESXi à l'aide des interfaces de ligne de commande de gestion de certificats disponibles pour la gestion des certificats vCenter Server.

Certificats dans vSphere 5.5 et dans vSphere 6.x

Lorsqu'ESXi et vCenter Server communiquent, ils utilisent les protocoles TLS/SSL pour presque l'ensemble du trafic de gestion.

Dans vSphere 5.5 et versions antérieures, les points de terminaison TLS/SSL sont sécurisés uniquement par une combinaison de nom d'utilisateur, mot de passe et empreinte. Les utilisateurs peuvent remplacer les certificats autosignés correspondants par leur propres certificats. Reportez-vous au Centre de documentation vSphere 5.5.

Dans vSphere 6.0 et versions ultérieures, vCenter Server prend en charge les modes de certificat suivants pour les hôtes ESXi.

Tableau 3-1. Modes de certificat des hôtes ESXi

Mode de certificat	Description
VMware Certificate Authority (par défaut)	Utilisez ce mode si VMCA provisionne tous les hôtes ESXi, comme autorité de certification de niveau supérieur ou comme autorité de certification intermédiaire. Par défaut, VMCA provisionne les hôtes ESXi avec des certificats. Dans ce mode, vous pouvez actualiser et renouveler les certificats dans vSphere Web Client.
Autorité de certification personnalisée	Utilisez ce mode si vous souhaitez uniquement utiliser des certificats personnalisés qui sont signés par une autorité de certification tierce ou de l'entreprise. Dans ce mode, vous êtes responsable de la gestion des certificats. Vous ne pouvez pas actualiser et renouveler des certificats dans vSphere Web Client. **Remarque** Sauf si vous définissez le mode de certificat sur Autorité de certification personnalisée, VMCA peut remplacer des certificats personnalisés, notamment lorsque vous sélectionnez **Renouveler** dans vSphere Web Client.
Mode d'empreinte	vSphere 5.5 utilisait le mode empreinte numérique. Ce mode reste disponible en tant qu'option de repli pour vSphere 6.x. Dans ce mode, vCenter Server s'assure que le certificat est formaté correctement, mais ne vérifie pas sa validité. Même les certificats expirés sont acceptés. N'utilisez ce mode que si vous rencontrez des problèmes que vous ne pouvez pas résoudre avec l'un des deux autres modes. Certains services vCenter 6.x et versions ultérieures ne fonctionnent pas correctement en mode d'empreinte.

Expiration du certificat

À partir de vSphere 6.0, vous pouvez afficher des informations sur l'expiration des certificats qui sont signés par VMCA ou par une autorité de certification tierce dans vSphere Web Client. Vous pouvez afficher les informations de tous les hôtes qui sont gérés par un système vCenter Server ou les informations d'hôtes individuels. Une alarme jaune se déclenche si le certificat est dans l'état **Expiration prochaine** (inférieure à huit mois). Une alarme rouge se déclenche si le certificat est dans l'état **Expiration imminente** (inférieure à deux mois).

Provisionnement d' ESXi et VMCA

Lorsque vous démarrez un hôte ESXi à partir d'un support d'installation, l'hôte dispose initialement d'un certificat automatiquement généré. Lorsque l'hôte est ajouté au système vCenter Server, il est provisionné avec un certificat signé par VMCA comme autorité de certification racine.

Le processus est similaire pour les hôtes qui sont provisionnés avec Auto Deploy. Cependant, comme ces hôtes ne stockent pas d'état, le certificat signé est stocké par le serveur Auto Deploy dans son magasin de certificats local. Le certificat est réutilisé lors des démarrages suivants des hôtes ESXi. Un serveur Auto Deploy fait partie d'un déploiement intégré ou d'un système vCenter Server.

Si VMCA n'est pas disponible lorsqu'un hôte Auto Deploy démarre pour la première fois, l'hôte tente de se connecter en premier lieu. Si cet hôte ne peut pas se connecter, il alterne les arrêts et les redémarrages jusqu'à ce que VMCA devienne disponible et que l'hôte soit provisionné avec un certificat signé.

Privilèges requis pour la gestion des certificats de ESXi

Pour la gestion des certificats des hôtes ESXi, vous devez disposer du privilège**Certificats.Gérer des certificats**. Vous pouvez définir ce privilège à partir de vSphere Web Client.

Modifications de nom d'hôte et d'adresse IP

Dans vSphere 6.0 et versions ultérieures, une modification de nom d'hôte ou d'adresse IP peut déterminer si vCenter Server considère valide le certificat d'un hôte. Le mode d'ajout de l'hôte à vCenter Server détermine si une intervention manuelle est nécessaire. Lors d'une intervention manuelle, vous reconnectez l'hôte, ou vous le supprimez de vCenter Server et le rajoutez.

Tableau 3-2. Quand des modifications de nom d'hôte ou d'adresse IP nécessitent-elles une intervention manuelle ?

Hôte ajouté à vCenter Server à l'aide de...	Modifications de nom d'hôte	Modifications d'adresse IP
Nom d'hôte	Problème de connectivité de vCenter Server. Intervention manuelle requise.	Aucune intervention requise.
Adresse IP	Aucune intervention requise.	Problème de connectivité de vCenter Server. Intervention manuelle requise.

Gestion des certificats ESXi (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_esxi_certs_in_vsphere)

Mises à niveau d'hôtes et certificats

Si vous mettez à niveau un hôte ESXi vers ESXi 6.0 ou version ultérieure, le processus de mise à niveau remplace les certificats auto-signés (empreinte) par des certificats signés par VMCA. Si l'hôte ESXi utilise des certificats personnalisés, le processus de mise à niveau conserve ces certificats même s'ils sont expirés ou non valides.

Si vous décidez de ne pas mettre à niveau vos hôtes vers ESXi 6.0 ou version ultérieure, les hôtes conservent les certificats que vous utilisez actuellement même si l'hôte est géré par un système vCenter Server qui utilise des certificats VMCA.

Le workflow de mise à niveau recommandé dépend des certificats actuels.

Hôte provisionné avec des certificats d'empreinte

Si votre hôte utilise actuellement des certificats d'empreinte, des certificats VMCA lui sont automatiquement attribués dans le cadre du processus de mise à niveau.

Remarque Vous ne pouvez pas provisionner des hôtes hérités avec des certificats VMCA. Vous devrez plus tard mettre à niveau ces hôtes vers ESXi 6.0.

Hôte provisionné avec des certificats personnalisés

Si votre hôte est provisionné avec des certificats personnalisés, généralement des certificats signés par une autorité de certification tierce, ces certificats restent en place pendant la mise à niveau. Optez pour le mode de certificat **Personnalisé** pour garantir que les certificats ne sont pas remplacés accidentellement lors d'une actualisation de certificats ultérieure.

Remarque Si votre environnement est en mode VMCA et que vous actualisez les certificats dans vSphere Web Client, tous les certificats existants sont remplacés par des certificats signés par VMCA.

Par la suite, vCenter Server surveille les certificats et affiche des informations, notamment sur l'expiration des certificats, dans vSphere Web Client.

Hôtes provisionnés avec Auto Deploy

Les hôtes qui sont provisionnés par Auto Deploy obtiennent toujours de nouveaux certificats lors de leur premier démarrage avec le logiciel ESXi 6.0 ou version ultérieure. Lorsque vous mettez à niveau un hôte qui est provisionné par Auto Deploy, le serveur Auto Deploy génère une demande de signature de certificat (CSR) pour l'hôte et la soumet à VMCA. VMCA stocke le certificat signé pour l'hôte. Lorsque le serveur Auto Deploy provisionne l'hôte, il récupère le certificat de VMCA et l'inclut dans le cadre du processus de provisionnement.

Vous pouvez utiliser Auto Deploy avec des certificats personnalisés.

Reportez-vous à « Utiliser des certificats personnalisés avec Auto Deploy », page 65.

Workflows de changement mode de certificat

À partir de vSphere 6.0, les hôtes ESXi sont provisionnés avec des certificats par VMCA par défaut. Vous devez plutôt utiliser le mode de certification personnalisée ou, à des fins de débogage, le mode d'empreinte hérité. Dans la plupart des cas, les changements de mode sont perturbateurs et ne sont pas nécessaires. Si un changement de mode s'impose, évaluez l'impact potentiel avant de commencer.

Dans vSphere 6.0 et versions ultérieures, vCenter Server prend en charge les modes de certificat suivants pour les hôtes ESXi.

Mode de certificat	Description
VMware Certificate Authority (par défaut)	Par défaut, VMware Certificate Authority est utilisée comme autorité de certification pour les certificats des hôtes ESXi. VMCA est l'autorité de certification racine par défaut, mais elle peut être définie comme autorité de certification intermédiaire vers une autre autorité de certification. Dans ce mode, les utilisateurs peuvent gérer des certificats dans vSphere Web Client. Ce mode est également utilisé si VMCA est un certificat subordonné.
Autorité de certification personnalisée	Certains clients préfèrent gérer leur propre autorité de certification externe. Dans ce mode, les clients sont responsables de la gestion des certificats et ne peuvent pas les gérer depuis vSphere Web Client.
Mode d'empreinte	vSphere 5.5 utilisait le mode d'empreinte et ce mode reste disponible en tant qu'option de repli pour vSphere 6.0. Toutefois, n'utilisez pas ce mode en cas de problèmes avec l'un ou les deux autres modes que vous ne pouvez pas résoudre. Certains services vCenter 6.0 et versions ultérieures ne fonctionnent pas correctement en mode d'empreinte.

Utilisation de certificats ESXi personnalisés

Si la stratégie de votre entreprise impose l'utilisation d'une autorité de certification racine autre que VMCA, vous pouvez changer le mode de certification de votre environnement après avoir procédé à une planification rigoureuse. Le workflow recommandé est le suivant.

1 Obtenez les certificats que vous souhaitez utiliser.

2 Retirez tous les hôtes du serveur vCenter Server.

3 Ajoutez le certificat racine de l'autorité de certification personnalisée dans VECS (VMware Endpoint Certificate Store).

4 Déployez les certificats de l'autorité de certification personnalisée sur chaque hôte et redémarrez les services sur cet hôte.

5 Passez au mode d'autorité de certification personnalisée. Reportez-vous à « Changer le mode de certificat », page 61.

6 Ajoutez les hôtes au système vCenter Server.

Passage du mode d'autorité de certification personnalisée au mode VMCA

Si vous utilisez le mode d'autorité de certification personnalisée et en venez à la conclusion que VMCA fonctionne mieux dans votre environnement, vous pouvez procéder au changement de mode après une planification rigoureuse. Le workflow recommandé est le suivant.

1 Retirez tous les hôtes du système vCenter Server.

2 Sur le système vCenter Server, retirez de VECS le certificat racine de l'autorité de certification tierce.

3 Passez au mode VMCA. Reportez-vous à « Changer le mode de certificat », page 61.

4 Ajoutez les hôtes au système vCenter Server.

Remarque Tout autre workflow pour ce mode peut entraîner un comportement imprévisible.

Conservation des certificats du mode d'empreinte pendant la mise à niveau

Le passage du mode VMCA au mode d'empreinte peut être nécessaire si vous rencontrez des problèmes avec les certificats VMCA. En mode d'empreinte, le système vCenter Server vérifie uniquement la présence et le format d'un certificat, mais pas sa validitié. Voir « Changer le mode de certificat », page 61 pour plus d'informations.

Passage du mode d'empreinte au mode VMCA

Si vous utilisez le mode d'empreinte et que vous souhaitez commencer à utiliser des certificats signés par VMCA, le changement nécessite de la planification. Le workflow recommandé est le suivant.

1 Retirez tous les hôtes du système vCenter Server.

2 Passez au mode de certification VMCA. Reportez-vous à « Changer le mode de certificat », page 61.

3 Ajoutez les hôtes au système vCenter Server.

Remarque Tout autre workflow pour ce mode peut entraîner un comportement imprévisible.

Passage du mode d'autorité de certification personnalisé au mode d'empreinte

Si vous rencontrez des problèmes avec votre autorité de certification personnalisée, envisagez de passer temporairement au mode d'empreinte. Le changement s'effectue de façon transparente si vous suivez les instructions de la section « Changer le mode de certificat », page 61. Après le changement de mode, le système vCenter Server vérifie uniquement le format du certificat et ne vérifie plus la validité du certificat proprement dit.

Passage du mode d'empreinte au mode d'autorité de certification personnalisée

Si vous définissez votre environnement sur le mode d'empreinte pendant un dépannage et que vous souhaitez commencer à utiliser le mode d'autorité de certification personnalisée, vous devez d'abord générer les certificats requis. Le workflow recommandé est le suivant.

1 Retirez tous les hôtes du système vCenter Server.

2 Ajoutez le certificat racine de l'autorité de certification personnalisée au magasin TRUSTED_ROOTS dans VECS sur le système vCenter Server. Reportez-vous à « Mettre à jour le magasin TRUSTED_ROOTS de vCenter Server (Certificats personnalisés) », page 64.

3 Pour chaque hôte ESXi :

   a Déployez le certificat et la clé de l'autorité de certification personnalisée.

   b Redémarrez les services sur l'hôte.

4 Passez au mode personnalisé. Reportez-vous à « Changer le mode de certificat », page 61.

5 Ajoutez les hôtes au système vCenter Server.

Paramètres par défaut des certificats ESXi

Lorsqu'un hôte est ajouté à un système vCenter Server, vCenter Server envoie une demande de signature de certificat (CSR) pour l'hôte à VMCA. La plupart des valeurs par défaut conviennent à de nombreuses situations, mais les informations spécifiques à l'entreprise peuvent être modifiées.

Vous pouvez modifier un grand nombre des paramètres par défaut à l'aide de vSphere Web Client. Envisagez de changer les informations sur l'entreprise et l'emplacement. Reportez-vous à « Modifier les paramètres par défaut de certificat », page 58.

Tableau 3-3. Paramètres CSR ESXi

Paramètre	Valeur par défaut	Option avancée
Taille de la clé	2048	S.O.
Algorithme de clé	RSA	S.O.
Algorithme de signature de certificat	sha256WithRSAEncryption	S.O.

Tableau 3-3. Paramètres CSR ESXi (suite)

Paramètre	Valeur par défaut	Option avancée
Nom commun	Nom de l'hôte si ce dernier a été ajouté à vCenter Server par nom d'hôte. Adresse IP de l'hôte si ce dernier a été ajouté à vCenter Server par adresse IP.	S.O.
Pays	États-Unis	vpxd.certmgmt.certs.cn.country
Adresse e-mail	vmca@vmware.com	vpxd.certmgmt.certs.cn.email
Localité (ville)	Palo Alto	vpxd.certmgmt.certs.cn.localityName
Nom d'unité d'organisation	VMware Engineering	vpxd.certmgmt.certs.cn.organizationalUnitName
Nom de l'organisation	VMware	vpxd.certmgmt.certs.cn.organizationName
État ou province	Californie	vpxd.certmgmt.certs.cn.state
Nombre de jours de validité du certificat.	1825	vpxd.certmgmt.certs.cn.daysValid
Seuil fixe d'expiration du certificat. vCenter Server génère une alarme rouge lorsque ce seuil est atteint.	30 jours	vpxd.certmgmt.certs.cn.hardThreshold
Intervalle d'interrogation des vérifications de la validité des certificats de vCenter Server.	5 jours	vpxd.certmgmt.certs.cn.pollIntervalDays
Seuil dynamique d'expiration du certificat. vCenter Server génère un événement lorsque ce seuil est atteint.	240 jours	vpxd.certmgmt.certs.cn.softThreshold
Mode employé par les utilisateurs de vCenter Server pour déterminer si les certificats existants sont remplacés. Modifiez ce mode pour conserver les certificats personnalisés pendant la mise à niveau. Reportez-vous à « Mises à niveau d'hôtes et certificats », page 54.	La valeur par défaut est vmca. Vous pouvez également spécifier Empreinte ou Personnalisé. Reportez-vous à « Changer le mode de certificat », page 61.	vpxd.certmgmt.mode

Modifier les paramètres par défaut de certificat

Lorsqu'un hôte est ajouté à un système vCenter Server, vCenter Server envoie une demande de signature de certificat (CSR) pour l'hôte à VMCA. Vous pouvez modifier certains paramètres par défaut dans la demande CSR en utilisant les paramètres avancés de vCenter Server dans vSphere Web Client.

Modifiez les paramètres par défaut du certificat spécifiques à l'entreprise. Reportez-vous à « Paramètres par défaut des certificats ESXi », page 57 pour obtenir la liste complète des paramètres par défaut. Certaines valeurs par défaut ne peuvent pas être modifiées.

Procédure

1 Dans vSphere Web Client, sélectionnez le système vCenter Server qui gère les hôtes.

2 Cliquez sur **Configurer**, puis sur **Paramètres avancés**.

3 Dans la zone Filtre, entrez **`certmgmt`** pour afficher uniquement les paramètres de gestion des certificats.

4 Modifiez la valeur des paramètres existants pour appliquer la stratégie de l'entreprise, puis cliquez sur **OK**.

Lors du prochain ajout d'un hôte à vCenter Server, les nouveaux paramètres seront utilisés dans la demande CSR que vCenter Server enverra à VMCA et dans le certificate attribué à l'hôte.

Suivant

Les modifications apportées aux métadonnées des certificats affectent uniquement les nouveaux certificats. Si vous souhaitez modifier les certificats d'hôtes déjà gérés par le système vCenter Server, vous pouvez déconnecter et reconnecter les hôtes, ou renouveler les certificats.

Afficher les informations d'expiration de certificat pour plusieurs hôtes ESXi

Si vous utilisez ESXi 6.0 ou version ultérieure, vous pouvez afficher l'état du certificat de tous les hôtes gérés par votre système vCenter Server. Cet affichage vous permet de déterminer si l'un des certificats est sur le point d'expirer.

Vous pouvez afficher des informations sur l'état d'un certificat pour les hôtes qui utilisent le mode VMCA, ainsi que pour ceux qui utilisent le mode personnalisé dans vSphere Web Client. Il n'est pas possible d'afficher des informations sur l'état du certificat pour les hôtes en mode Empreinte.

Procédure

1 Accédez à l'hôte dans la hiérarchie de l'inventaire de vSphere Web Client.

Par défaut, l'affichage des hôtes n'inclut pas l'état du certificat.

2 Cliquez avec le bouton droit sur le champ Nom et sélectionnez l'option **Afficher/masquer les colonnes**.

3 Sélectionnez **Certificat valide pour**, cliquez sur **OK** et faites défiler vers la droite, si nécessaire.

Les informations relatives au certificat s'affichent lorsque le certificat expire.

Si un hôte est ajouté à vCenter Server ou reconnecté après une déconnexion, vCenter Server renouvelle le certificat si son état est Expiré, Expiration, Expiration prochaine ou Expiration imminente. L'état est Expiration si la validité du certificat est inférieure à huit mois, Expiration prochaine si la validité est inférieure à deux mois et Expiration imminente si elle est inférieure à un mois.

4 (Facultatif) Désélectionnez les autres colonnes pour faciliter l'observation de ce qui vous intéresse.

Suivant

Renouvelez les certificats qui sont sur le point d'expirer. Reportez-vous à « Renouveler ou actualiser des certificats ESXi », page 60.

Afficher les détails de certificat pour un hôte ESXi spécifique

Pour les hôtes ESXi 6.0 et versions ultérieures qui sont en mode VMCA ou en mode personnalisé, vous pouvez afficher les détails du certificat dans vSphere Web Client. Les informations sur le certificat peuvent être utiles lors d'un débogage.

Procédure

1 Accédez à l'hôte dans l'inventaire de vSphere Web Client.

2 Sélectionnez **Configurer**.

3 Sous **Système**, cliquez sur **Certificat**.

Vous pouvez afficher les informations suivantes. Ces informations sont disponibles uniquement dans la vue d'hôte unique.

Champ	Description	
Objet	Objet utilisé lors de la génération du certificat.	
Émetteur	Émetteur du certificat.	
Date de début de validité	Date à laquelle le certificat a été généré.	
Date de fin de validité	Date à laquelle le certificat expire.	
État	État du certificat, à savoir l'un des états suivants.	
	Bon	Fonctionnement normal.
	Expiration	Le certificat va bientôt expirer.
	Expiration imminente	La date d'expiration du certificat se situe dans huit mois ou moins (par défaut).
	Expiration imminente	Le certificat se situe à 2 mois ou moins de sa date d'expiration (par défaut).
	Expiré	Le certificat n'est pas valide, car il a expiré.

Renouveler ou actualiser des certificats ESXi

Si l'autorité de certification VMware (VMCA) attribue des certificats à vos hôtes ESXi (6.0 et version ultérieure), vous pouvez renouveler ces certificats à partir de vSphere Web Client. Vous pouvez également actualiser tous les certificats du magasin TRUSTED_ROOTS associés à vCenter Server.

Vous pouvez renouveler vos certificats lorsqu'ils sont sur le point d'expirer ou si vous souhaitez provisionner l'hôte avec un nouveau certificat pour d'autres raisons. Si le certificat a déjà expiré, vous devez déconnecter puis reconnecter l'hôte.

Par défaut, vCenter Server renouvelle les certificats des hôtes dont l'état est Expiré, Expire immédiatement ou Expiration chaque fois que l'hôte est ajouté à l'inventaire ou qu'il est reconnecté.

Procédure

1 Accédez à l'hôte dans l'inventaire de vSphere Web Client.

2 Sélectionnez **Configurer**.

3 Sous **Système**, cliquez sur **Certificat**.

Il est possible d'afficher des informations détaillées sur le certificat de l'hôte sélectionné.

4 Cliquez sur **Renouveler** ou sur **Actualiser les certificats d'autorité de certification**.

Option	Description
Renouveler	Récupère, auprès de l'autorité de certification VMware (VMCA), un certificat venant d'être signé pour l'hôte.
Actualiser les certificats d'autorité de certification	Pousse tous les certificats du magasin TRUSTED_ROOTS dans le magasin VECS de vCenter Server vers l'hôte.

5 Cliquez sur **Oui** pour confirmer.

Changer le mode de certificat

Dans la plupart des cas, la meilleure solution consiste à utiliser VMCA pour provisionner les hôtes ESXi dans votre environnement. Si la stratégie de l'entreprise exige que vous utilisiez des certificats personnalisés avec une autorité de certification racine différente, vous pouvez modifier les options avancées de vCenter Server afin d'éviter que les hôtes soient automatiquement provisionnés à l'aide de certificats VMCA lorsque vous actualisez les certificats. Vous êtes alors responsable de la gestion des certificats dans votre environnement.

Vous pouvez utiliser les paramètres avancés de vCenter Server pour passer au mode d'empreinte ou d'autorité de certification personnalisée. N'utilisez le mode d'empreinte que comme option de secours.

Procédure

1 Sélectionnez le système vCenter Server qui gère les hôtes et cliquez sur **Configurer**.

2 Cliquez sur **Paramètres avancés**, puis sur **Modifier**.

3 Dans le champ Filtre, entrez **`certmgmt`** pour afficher uniquement les clés de gestion des certificats.

4 Définissez vpxd.certmgmt.mode sur **personnalisé** si vous souhaitez gérer vos propres certificats ou sur **empreinte** si vous préférez utiliser temporairement le mode d'empreinte, puis cliquez sur **OK**.

5 Redémarrez le service vCenter Server.

Remplacement de certificats et de clés SSL pour ESXi

Selon la stratégie de sécurité de votre entreprise, vous devrez peut-être remplacer le certificat SSL défini par défaut pour ESXi par un certificat signé par une autorité de certification tierce sur chaque hôte.

Par défaut, les composants vSphere utilisent le certificat signé par VMCA et la clé créés lors de l'installation. Si vous supprimez accidentellement le certificat signé par VMCA, supprimez l'hôte de son système vCenter Server, puis ajoutez-le de nouveau. Lorsque vous ajoutez l'hôte, vCenter Server demande un nouveau certificat à VMCA et provisionne l'hôte à l'aide de celui-ci.

Si la stratégie de l'entreprise l'impose, remplacez les certificats signés par VMCA par des certificats provenant d'une autorité de certification approuvée (une autorité de certification commerciale ou l'autorité de certification d'une organisation).

Les certificats par défaut se trouvent au même emplacement que les certificats vSphere 5.5. Vous pouvez remplacer de plusieurs manières les certificats par défaut par des certificats approuvés.

Remarque Vous pouvez également utiliser les objets gérés `vim.CertificateManager` et `vim.host.CertificateManager` dans vSphere Web Services SDK. Reportez-vous à la documentation vSphere Web Services SDK.

Après avoir remplacé le certificat, vous devez mettre à jour le magasin TRUSTED_ROOTS dans VECS sur le système vCenter Server qui gère l'hôte, afin de garantir une relation de confiance entre vCenter Server et l'hôte ESXi.

- Configuration requise pour les demandes de signature de certificat ESXi page 62

  Si vous souhaitez utiliser un certificat d'entreprise ou signé par une autorité de certification tierce, vous devez envoyer une demande de signature de certificat (CRS) à l'autorité de certification.

- Remplacer le certificat et la clé par défaut dans ESXi Shell page 62

  Vous pouvez remplacer les certificats ESXi signés par VMCA par défaut dans ESXi Shell.

- Remplacer un certificat et une clé par défaut à l'aide de la commande vifs page 63

  Vous pouvez remplacer les certificats ESXi par défaut signés par VMware Certificate Authority (VMCA) à l'aide de la commande `vifs`.

- Remplacer un certificat par défaut à l'aide de HTTPS PUT page 64

  Vous pouvez utiliser des applications tierces pour télécharger des certificats et une clé. Les applications prenant en charge les opérations HTTPS PUT utilisent l'interface HTTPS incluse avec ESXi.

- Mettre à jour le magasin TRUSTED_ROOTS de vCenter Server (Certificats personnalisés) page 64

  Si vous configurez vos hôtes ESXi pour qu'ils utilisent des certificats personnalisés, vous devez mettre à niveau le magasin `TRUSTED_ROOTS` du système vCenter Server qui gère les hôtes.

Configuration requise pour les demandes de signature de certificat ESXi

Si vous souhaitez utiliser un certificat d'entreprise ou signé par une autorité de certification tierce, vous devez envoyer une demande de signature de certificat (CRS) à l'autorité de certification.

Utilisez une demande de signature de certificat présentant les caractéristiques suivantes :

- Taille de clé : 2 048 bits ou plus (codée au format PEM)
- Format PEM. VMware prend en charge PKCS8 et PKCS1 (clés RSA). Lorsque des clés sont ajoutées à VECS, elles sont converties en PKCS8
- x509 version 3
- Pour les certificats racines, l'extension d'autorité de certification doit être définie sur true et la signature de certification doit figurer dans la liste de conditions requises.
- SubjectAltName doit contenir DNS Name=<machine_FQDN>
- Format CRT
- Contient les utilisations de clé suivantes : signature numérique, non-répudiation, chiffrement de la clé
- Heure de début antérieure d'un jour à l'heure actuelle
- CN (et SubjectAltName) défini sur le nom de l'hôte (ou l'adresse IP) de l'hôte ESXi dans l'inventaire vCenter Server.

Remplacer le certificat et la clé par défaut dans ESXi Shell

Vous pouvez remplacer les certificats ESXi signés par VMCA par défaut dans ESXi Shell.

Prérequis

- Si vous souhaitez utiliser des certificats signés par une autorité de certification tierce, générez la demande de certificat, envoyez-la à l'autorité de certification et stockez les certificats sur chaque hôte ESXi.
- Si nécessaire, activez ESXi Shell ou activez le trafic SSH dans vSphere Web Client. Consultez la publication *Sécurité vSphere* pour plus d'informations sur l'activation de l'accès à ESXi Shell.
- Tous les transferts de fichiers et autres communications se produisent lors d'une session HTTPS sécurisée. L'utilisateur servant à authentifier la session doit disposer du privilège **Hôte.Config.AdvancedConfig** sur l'hôte. Consultez la publication *Sécurité vSphere* pour plus d'informations sur l'attribution de privilèges par le biais de rôles.

Procédure

1 Connectez-vous à ESXi Shell, directement à partir de l'interface utilisateur de la console directe (DCUI) ou à partir d'un client SSH, en tant qu'utilisateur disposant de privilèges d'administrateur.

2 Dans l'inventaire `/etc/vmware/ssl`, renommer les certificats existants à l'aide des commandes suivantes :

```
mv rui.crt orig.rui.crt
mv rui.key orig.rui.key
```

3 Copiez les certificats à utiliser dans `/etc/vmware/ssl`.

4 Renommer le nouveau certificat et la clé dans `rui.crt` et `rui.key`.

5 Redémarrez l'hôte après avoir installé le nouveau certificat.

Vous pouvez également mettre l'hôte en mode de maintenance, installer le nouveau certificat, utiliser l'interface utilisateur de console directe (DCUI) pour redémarrer les agents de gestion, puis configurer l'hôte pour quitter le mode de maintenance.

Suivant

Mettez à jour le magasin vCenter Server TRUSTED_ROOTS. Consultez la publication *Sécurité vSphere*.

Remplacer un certificat et une clé par défaut à l'aide de la commande vifs

Vous pouvez remplacer les certificats ESXi par défaut signés par VMware Certificate Authority (VMCA) à l'aide de la commande `vifs`.

Vous exécutez `vifs` comme commande vCLI. Reportez-vous à *Démarrage avec vSphere Command-Line Interfaces*.

.

Prérequis

- Si vous souhaitez utiliser des certificats signés par une autorité de certification tierce, générez la demande de certificat, envoyez-la à l'autorité de certification et stockez les certificats sur chaque hôte ESXi.
- Si nécessaire, activez ESXi Shell ou activez le trafic SSH dans vSphere Web Client. Consultez la publication *Sécurité vSphere* pour plus d'informations sur l'activation de l'accès à ESXi Shell.
- Tous les transferts de fichiers et autres communications se produisent lors d'une session HTTPS sécurisée. L'utilisateur servant à authentifier la session doit disposer du privilège **Hôte.Config.AdvancedConfig** sur l'hôte. Consultez la publication *Sécurité vSphere* pour plus d'informations sur l'attribution de privilèges par le biais de rôles.

Procédure

1 Sauvegardez les certificats existants.

2 Générez une demande de certificat en suivant les instructions de l'autorité de certification.

Reportez-vous à « Configuration requise pour les demandes de signature de certificat ESXi », page 62.

3 Lorsque vous avez le certificat, utilisez la commande `vifs` pour télécharger le certificat à l'emplacement approprié sur l'hôte à partir d'une connexion SSH vers l'hôte.

```
vifs --server nom_hôte --username nom_utilisateur --put rui.crt /host/ssl_cert
```

```
vifs --server nom_hôte --username nom_utilisateur --put rui.key /host/ssl_key
```

4 Redémarrez l'hôte.

Suivant

Mettez à jour le magasin vCenter Server TRUSTED_ROOTS. Reportez-vous à « Mettre à jour le magasin TRUSTED_ROOTS de vCenter Server (Certificats personnalisés) », page 64.

Remplacer un certificat par défaut à l'aide de HTTPS PUT

Vous pouvez utiliser des applications tierces pour télécharger des certificats et une clé. Les applications prenant en charge les opérations HTTPS PUT utilisent l'interface HTTPS incluse avec ESXi.

Prérequis

- Si vous souhaitez utiliser des certificats signés par une autorité de certification tierce, générez la demande de certificat, envoyez-la à l'autorité de certification et stockez les certificats sur chaque hôte ESXi.
- Si nécessaire, activez ESXi Shell ou activez le trafic SSH dans vSphere Web Client. Consultez la publication *Sécurité vSphere* pour plus d'informations sur l'activation de l'accès à ESXi Shell.
- Tous les transferts de fichiers et autres communications se produisent lors d'une session HTTPS sécurisée. L'utilisateur servant à authentifier la session doit disposer du privilège **Hôte.Config.AdvancedConfig** sur l'hôte. Consultez la publication *Sécurité vSphere* pour plus d'informations sur l'attribution de privilèges par le biais de rôles.

Procédure

1 Sauvegardez les certificats existants.

2 Dans votre application de téléchargement, traitez chaque fichier de la manière suivante :

   a Ouvrez le fichier.

   b Publiez le fichier à l'un de ces emplacements.

Option	Description
Certificats	`https://hostname/host/ssl_cert`
Clés	`https://hostname/host/ssl_key`

   Les emplacements `/host/ssl_cert` et `host/ssl_key` sont reliés aux fichiers de certificats dans `/etc/vmware/ssl`.

3 Redémarrez l'hôte.

Suivant

Mettez à jour le magasin TRUSTED_ROOTS de vCenter Server. Reportez-vous à « Mettre à jour le magasin TRUSTED_ROOTS de vCenter Server (Certificats personnalisés) », page 64.

Mettre à jour le magasin TRUSTED_ROOTS de vCenter Server (Certificats personnalisés)

Si vous configurez vos hôtes ESXi pour qu'ils utilisent des certificats personnalisés, vous devez mettre à niveau le magasin `TRUSTED_ROOTS` du système vCenter Server qui gère les hôtes.

Prérequis

Remplacez les certificats de chacun des hôtes par des certificats personnalisés.

Procédure

1 Connectez-vous au système vCenter Server qui gère les hôtes ESXi.

   Connectez-vous au système Windows sur lequel vous avez installé le logiciel ou au shell vCenter Server Appliance.

2 Exécutez `vecs-cli` pour ajouter les nouveaux certificats au magasin `TRUSTED_ROOTS`, par exemple :

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store TRUSTED_ROOTS --alias custom1.crt --
cert /etc/vmware/ssl/custom1.crt
```

Option	Description
Linux	`/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store TRUSTED_ROOTS --alias custom1.crt --cert /etc/vmware/ssl/custom1.crt`
Windows	`C:\Program Files\VMware\vCenter Server\vmafdd\vecs-cli entry create --store TRUSTED_ROOTS --alias custom1.crt --cert c:\ssl\custom1.crt`

Suivant

Définissez le mode de certificat sur Personnalisé. Si le mode de certificat est VMCA (c'est-à-dire la valeur par défaut) et que vous effectuez une actualisation des certificats, vos certificats personnalisés sont remplacés par des certificats signés par l'autorité de certification VMware (VMCA). Reportez-vous à « Changer le mode de certificat », page 61.

Utiliser des certificats personnalisés avec Auto Deploy

Par défaut, le serveur Auto Deploy provisionne chaque hôte avec des certificats signés par VMCA. Vous pouvez configurer le serveur Auto Deploy de manière à provisionner tous les hôtes à l'aide de certificats personnalisés non signés par VMCA. Dans ce scénario, le serveur Auto Deploy devient une autorité de certification subordonnée de l'autorité de certification tierce.

Prérequis

- Demandez un certificat à votre autorité de certification. Le certificat doit répondre aux conditions suivantes.
  - Taille de clé : 2 048 bits ou plus (codée au format PEM)
  - Format PEM. VMware prend en charge PKCS8 et PKCS1 (clés RSA). Lorsque des clés sont ajoutées à VECS, elles sont converties en PKCS8
  - x509 version 3
  - Pour les certificats racines, l'extension d'autorité de certification doit être définie sur true et la signature de certification doit figurer dans la liste de conditions requises.
  - SubjectAltName doit contenir DNS Name=<machine_FQDN>
  - Format CRT
  - Contient les utilisations de clé suivantes : signature numérique, non-répudiation, chiffrement de la clé
  - Heure de début antérieure d'un jour à l'heure actuelle
  - CN (et SubjectAltName) défini sur le nom de l'hôte (ou l'adresse IP) de l'hôte ESXi dans l'inventaire vCenter Server.
- Nom du certificat et fichiers de clés `rbd-ca.crt` et `rbd-ca.key`.

Procédure

1 Sauvegardez les certificats ESXi par défaut.

  Les certificats se situent à l'emplacement `/etc/vmware-rbd/ssl/`.

2 Dans vSphere Web Client, arrêtez le service Auto Deploy.

   a Sélectionnez **Administration**, puis cliquez sur **Configuration système** sous **Déploiement**.

   b Cliquez sur **Services**.

   c Cliquez avec le bouton droit sur le service que vous souhaitez arrêter et sélectionnez **Arrêter**.

3 Sur le système qui exécute le service Auto Deploy, dans `/etc/vmware-rbd/ssl/`, remplacez `rbd-ca.crt` et `rbd-ca.key` par votre certificat personnalisé et vos fichiers de clés.

4 Sur le système qui exécute le service Auto Deploy, mettez à jour le magasin TRUSTED_ROOTS dans VECS pour utiliser vos nouveaux certificats.

Option	Description

Windows	`cd C:\Program Files\VMware\vCenter Server\vmafdd\vecs-cli.exe`
	`vecs-cli entry delete --store TRUSTED_ROOTS --alias rbd_cert`
	`vecs-cli entry create --store TRUSTED_ROOTS --alias rbd_cert`
	`--cert /etc/vmware-rbd/ssl/rbd-ca.crt`

Linux	`cd /usr/lib/vmware-vmafd/bin/vecs-cli`
	`vecs-cli entry delete --store TRUSTED_ROOTS --alias rbd_cert`
	`vecs-cli entry create --store TRUSTED_ROOTS --alias rbd_cert`
	`--cert /etc/vmware-rbd/ssl/rbd-ca.crt`

5 Créez un fichier `castore.pem` contenant tout ce qui se trouve dans TRUSTED_ROOTS et placez-le dans le répertoire `/etc/vmware-rbd/ssl/`.

   En mode personnalisé, vous êtes responsable de la gestion de ce fichier.

6 Définissez le mode de certificat ESXi du système vCenter Server sur **`Personnalisé`**.

   Reportez-vous à « Changer le mode de certificat », page 61.

7 Redémarrez le service vCenter Server et démarrez le service Auto Deploy.

La prochaine fois que vous provisionnez un hôte configuré pour utiliser Auto Deploy, le serveur Auto Deploy génère un certificat. Le serveur Auto Deploy utilise le certificat racine que vous venez d'ajouter au magasin TRUSTED_ROOTS.

Restaurer les fichiers de certificat et de clé ESXi

Lorsque vous remplacez un certificat sur un hôte ESXi à l'aide de vSphere Web Services SDK, le certificat et la clé antérieurs sont ajoutés à un fichier `.bak`. Vous pouvez restaurer les certificats précédents en déplaçant les informations du fichier `.bak` vers les fichiers de certificat et de clé actuels.

Le certificat et la clé de l'hôte résident dans `/etc/vmware/ssl/rui.crt` et `/etc/vmware/ssl/rui.key`. Lorsque vous remplacez le certificat et la clé d'un hôte à l'aide de l'objet géré `vim.CertificateManager` de vSphere Web Services SDK, le certificat et la clé antérieurs sont ajoutés au fichier `/etc/vmware/ssl/rui.bak`.

Remarque Si vous remplacez le certificat à l'aide de HTTP PUT, `vifs` ou à partir d'ESXi Shell, les certificats existants ne sont pas ajoutés au fichier `.bak`.

Procédure

1 Sur l'hôte ESXi, accédez au fichier `/etc/vmware/ssl/rui.bak`.

Le format du fichier est le suivant :

```
#
# Host private key and certificate backup from 2014-06-20 08:02:49.961
#

-----BEGIN PRIVATE KEY-----
previous key
-----END PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
previous cert
-----END CERTIFICATE-----
```

2 Copiez le texte qui commence par `-----BEGIN PRIVATE KEY-----` et termine par `-----END PRIVATE KEY-----` dans le fichier `/etc/vmware/ssl/rui.clé`.

Incluez `-----BEGIN PRIVATE KEY-----` et `-----END PRIVATE KEY-----`.

3 Copiez le texte entre `-----BEGIN CERTIFICATE-----` et `-----END CERTIFICATE-----` dans le fichier `/etc/vmware/ssl/rui.crt`.

Incluez `-----BEGIN CERTIFICATE-----` et `-----END CERTIFICATE-----`.

4 Redémarrez l'hôte ou envoyez des événements `ssl_reset` à tous les services qui utilisent les clés.

```
for s in /etc/init.d/*; do $s | grep ssl_reset > /dev/null; if [ $? == 0 ]; then $s
ssl_reset; fi; done
```

Personnalisation des hôtes avec le profil de sécurité

Vous pouvez personnaliser la plupart des paramètres de sécurité essentiels de votre hôte via le panneau Profil de sécurité disponible dans vSphere Web Client. Le profil de sécurité est particulièrement utile pour la gestion d'hôte unique. Si vous gérez plusieurs hôtes, pensez à utiliser l'une des lignes de commande (CLI) ou l'un des kits de développement logiciel (SDK) et à automatiser la personnalisation.

ESXi

ESXi contient un pare-feu activé par défaut.

Lors de l'installation, le pare-feu d'ESXi est configuré pour bloquer le trafic entrant et sortant, sauf le trafic des services activés dans le profil de sécurité de l'hôte.

Réfléchissez bien avant d'ouvrir des ports sur le pare-feu, car l'accès illimité aux services qui s'exécutent sur un hôte ESXi peut exposer ce dernier aux attaques extérieures et aux accès non autorisés. Pour minimiser les risques, configurez le pare-feu ESXi de manière à autoriser l'accès uniquement depuis les réseaux autorisés.

Remarque Le pare-feu permet également d'utiliser les commandes ping ICMP (Internet Control Message Protocol) et autorise les communications avec les clients DHCP et DNS (UDP uniquement).

Vous pouvez gérer les ports du pare-feu d'ESXi de la manière suivante :

- Utilisez le profil de sécurité de chacun des hôtes dans vSphere Web Client. Reportez-vous à « Gérer les paramètres du pare-feu ESXi », page 68
- Utilisez les commandes ESXCLI dans la ligne de commande ou dans les scripts. Reportez-vous à « Commandes de pare-feu ESXCLI d'ESXi », page 73.

- Utilisez un VIB personnalisé si le port que vous cherchez à ouvrir n'est pas inclus dans le profil de sécurité.

  Vous créez des VIB personnalisés avec l'outil vibauthor disponible dans VMware Labs. Pour installer le VIB personnalisé, vous devez modifier le niveau d'acceptation de l'hôte ESXi sur CommunitySupported. Voir l'article 2007381 de la base de connaissances VMware.

  Remarque Si vous contactez le support technique VMware pour examiner un problème relatif à un hôte ESXi avec un VIB CommunitySupported installé, il se peut que le support VMware demande de désinstaller le VIB CommunitySupported dans le cadre de la résolution du problème afin de déterminer si ce VIB est associé au problème étudié.

Concepts du pare-feu d'ESXi (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_esxi_firewall_concepts)

Le comportement de l'ensemble de règles du client NFS (`nfsClient`) diffère de celui des autres ensembles de règles. Lorsque l'ensemble de règles du client NFS est activé, tous les ports TCP sortants sont ouverts aux hôtes de destination figurant dans la liste des adresses IP autorisées. Consultez « Comportement du pare-feu client NFS », page 72 pour plus d'informations.

Gérer les paramètres du pare-feu ESXi

Vous pouvez configurer les connexions de pare-feu entrantes et sortantes pour un agent de service ou de gestion dans vSphere Web Client ou sur la ligne de commande.

Remarque Si différents services ont des règles de port qui se chevauchent, l'activation d'un service peut implicitement activer d'autres services. Vous pouvez spécifier les adresses IP qui sont autorisées à accéder à chacun des services sur l'hôte afin d'éviter ce problème.

Procédure

1. Accédez à l'hôte dans l'inventaire de vSphere Web Client.
2. Cliquez sur **Configurer**.
3. Dans Système, cliquez sur **Profil de sécurité**.

   vSphere Web Client affiche la liste des connexions entrantes et sortantes actives avec les ports de pare-feu correspondants.
4. Dans la section Pare-feu, cliquez sur **Modifier**.

   L'écran affiche des ensembles de règles de pare-feu avec le nom de la règle et les informations associées.
5. Sélectionnez les ensembles de règles à activer, ou désélectionnez ceux à désactiver.

Colonne	Description
Ports entrants et port sortants	Les ports que vSphere Web Client ouvre pour le service
Protocole	Protocole utilisé par un service.
Processus	Statut des démons associés au service

6. Pour certains services, vous pouvez gérer les détails du service.
   - Utilisez les boutons **Démarrer**, **Arrêter** ou **Redémarrer** pour modifier temporairement l'état d'un service.
   - Modifier la stratégie de démarrage pour que le service démarre avec l'hôte ou avec l'utilisation du port.

7 Pour certains services, vous pouvez spécifier explicitement les adresses IP à partir desquelles les connexions sont autorisées.

Reportez-vous à « Ajouter des adresses IP autorisées pour un hôte ESXi », page 69.

8 Cliquez sur **OK**.

Ajouter des adresses IP autorisées pour un hôte ESXi

Par défaut, le pare-feu de chaque service autorise l'accès à toutes les adresses IP. Pour restreindre le trafic, modifiez chaque service pour autoriser uniquement le trafic provenant de votre sous-réseau de gestion. Vous pouvez également annuler la sélection de certains services si votre environnement ne les utilise pas.

Vous pouvez utiliser vSphere Web Client, vCLI ou PowerCLI pour mettre à jour la liste des adresses IP autorisées d'un service. Par défaut, toutes les adresses IP sont autorisées pour un service.

Ajout d'adresses IP autorisées au pare-feu ESXi (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_adding_allowed_IP_to_esxi_firewall)

Procédure

1 Accédez à l'hôte dans l'inventaire de vSphere Web Client.

2 Cliquez sur **Configurer**.

3 Dans Système, cliquez sur **Profil de sécurité**.

4 Dans la section Pare-feu, cliquez sur **Modifier**, puis sélectionnez un service dans la liste.

5 Dans la section Adresses IP autorisées, désélectionnez **Autoriser les connexions de toutes les adresses IP**, puis saisissez les adresses IP des réseaux autorisés à se connecter à l'hôte.

Séparez les adresses IP avec des virgules. Vous pouvez utiliser les formats d'adresse suivants :

- 192.168.0.0/24
- 192.168.1.2, 2001::1/64
- fd3e:29a6:0a81:e478::/64

6 Cliquez sur **OK**.

Ports de pare-feu entrants et sortants pour les hôtes ESXi

vSphere Web Client et VMware Host Client vous permettent d'ouvrir et de fermer les ports de pare-feu pour chaque service ou encore d'autoriser le trafic provenant d'adresses IP sélectionnées.

Le tableau ci-dessous répertorie les pare-feu pour les services généralement installés. Il est possible de disposer de services et de ports de pare-feu supplémentaires en installant d'autres VIB sur l'hôte. Ces informations s'adressent principalement aux services visibles dans vSphere Web Client mais le tableau inclut aussi d'autres ports.

Tableau 3-4. Connexions de pare-feu entrantes

Port	Protocole	Service	Description
5988	TCP	Serveur CIM	Serveur pour CIM (Common Information Model).
5989	TCP	Serveur sécurisé CIM	Serveur sécurisé pour CIM.
427	TCP, UDP	SLP CIM	Le client CIM utilise le Service Location Protocol, version 2 (SLPv2) pour rechercher des serveurs CIM.
546		DHCPv6	Client DHCP pour IPv6.

Tableau 3-4. Connexions de pare-feu entrantes (suite)

Port	Protocole	Service	Description
8301, 8302	UDP	DVSSync	Les ports DVSSync permettent de synchroniser les états des ports virtuels distribués entre les hôtes pour lesquels l'enregistrement et la lecture VMware FT sont activés. Seuls les ports des hôtes qui exécutent des machines virtuelles principales ou de sauvegarde doivent être ouverts. Sur les ports qui n'utilisent pas VMware FT, ces ports n'ont pas besoin d'être ouverts.
902	TCP	NFC	La NFC (Network File Copy, copie de fichiers réseau) fournit un service FTP capable de reconnaître les types de fichiers pour les composants vSphere. ESXi utilise par défaut la technologie NFC pour des opérations comme la copie ou le transfert de données entre banques de données.
12345, 23451	UDP	Service de clustering Virtual SAN	Service d'annuaire pour l'adhésion au cluster Virtual SAN et la surveillance de ce dernier. Utilise la multidifusion IP basée sur UDP pour établir les membres du cluster et distribuer les métadonnées Virtual SAN à tous les membres du cluster. Si ce service est désactivé, Virtual SAN ne fonctionne pas.
68	UDP	Client DHCP	Client DHCP pour IPv4.
53	UDP	Client DNS	Client DNS.
8200, 8100, 8300	TCP, UDP	Fault Tolerance	Trafic entre les hôtes pour vSphere Fault Tolerance (FT).
6999	UDP	Service de routeur logique distribué NSX	Service de routeur distribué virtuel NSX. Le port de pare-feu associé à ce service est ouvert lorsque les VIB NSX sont installés et que le module VDR (Virtual Distributed Router) est créé. Si aucune instance de VDR n'est associée à l'hôte, le port n'a pas besoin d'être ouvert. Ce service s'appelait « Service de routeur logique distribué NSX » dans les versions précédentes du produit.
2233	TCP	Transport Virtual SAN	Transport de datagramme fiable pour Virtual SAN. Exploite TCP et est employé pour les E/S de stockage Virtual SAN. Si ce service est désactivé, Virtual SAN ne fonctionne pas.
161	UDP	Serveur SNMP	Permet à l'hôte de se connecter à un serveur SNMP.
22	TCP	Serveur SSH	Requis pour l'accès SSH.
8000	TCP	vMotion	Requis pour la migration de machines virtuelles avec vMotion. Les hôtes ESXi écoutent sur le port 8000 pour les connexions TCP à partir des hôtes ESXi distants pour le trafic vMotion.
902, 443	TCP	vSphere Web Client	Connexions client
8080	TCP	vsanvp	Fournisseur de distributeur VSAN VASA. Utilisé pour le service de gestion du stockage (SMS) inclus dans vCenter pour accéder aux informations relatives à la conformité, aux capacités et aux profils de stockage Virtual SAN. Si le service est désactivé, Virtual SAN Storage Profile Based Management (SPBM) ne fonctionne pas.
80	TCP	vSphere Web Access	Page de bienvenue, avec liens de téléchargement pour différentes interfaces.
5900-5964	TCP	Protocole RFB	
80, 9000	TCP	vSphere Update Manager	

Tableau 3-5. Connexions de pare-feu sortantes

Port	Protocole	Service	Description
427	TCP, UDP	SLP CIM	Le client CIM utilise le Service Location Protocol, version 2 (SLPv2) pour rechercher des serveurs CIM.
547	TCP, UDP	DHCPv6	Client DHCP pour IPv6.
8301, 8302	UDP	DVSSync	Les ports DVSSync permettent de synchroniser les états des ports virtuels distribués entre les hôtes pour lesquels l'enregistrement et la lecture VMware FT sont activés. Seuls les ports des hôtes qui exécutent des machines virtuelles principales ou de sauvegarde doivent être ouverts. Sur les ports qui n'utilisent pas VMware FT, ces ports n'ont pas besoin d'être ouverts.
44046, 31031	TCP	HBR	Utilisé par vSphere Replication et VMware Site Recovery Manager pour le trafic de réplication en cours.
902	TCP	NFC	La NFC (Network File Copy, copie de fichiers réseau) fournit un service FTP capable de reconnaître les types de fichiers pour les composants vSphere. ESXi utilise par défaut la technologie NFC pour des opérations comme la copie ou le transfert de données entre banques de données.
9	UDP	WOL	Utilisé par Réveil sur réseau local LAN.
12345 23451	UDP	Service de clustering Virtual SAN	Surveillance du cluster, appartenance et service d'annuaire utilisé par Virtual SAN.
68	UDP	Client DHCP	Client DHCP.
53	TCP, UDP	Client DNS	Client DNS.
80, 8200, 8100, 8300	TCP, UDP	Fault Tolerance	Prend en charge VMware Fault Tolerance.
3260	TCP	Client de logiciel iSCSI	Prend en charge l'iSCSI logiciel.
6999	UDP	Service de routeur logique distribué NSX	Le port de pare-feu associé à ce service est ouvert lorsque les VIB NSX sont installés et que le module VDR (Virtual Distributed Router) est créé. Si aucune instance de VDR n'est associée à l'hôte, le port n'a pas besoin d'être ouvert.
5671	TCP	rabbitmqproxy	Proxy s'exécutant sur l'hôte ESXi, qui permet aux applications exécutées sur des machines virtuelles de communiquer avec les brokers AMQP qui s'exécutent dans le domaine réseau de vCenter. Il n'est pas nécessaire que la machine virtuelle se trouve sur le réseau. En d'autres termes, aucune carte réseau n'est requise. Le proxy se connecte aux brokers dans le domaine de réseau vCenter. Par conséquent, les adresses IP des connexions sortantes doivent inclure au moins les brokers actuellement utilisés ou les futurs brokers. Si un client souhaite monter en charge, il est possible d'ajouter des brokers.
2233	TCP	Transport Virtual SAN	Utilisé pour le trafic RDT (communication monodiffusion de poste à poste) entre nœuds Virtual SAN.
8000	TCP	vMotion	Requis pour la migration de machines virtuelles avec vMotion.
902	UDP	Agent VMware vCenter	Agent vCenter Server.

Tableau 3-5. Connexions de pare-feu sortantes (suite)

Port	Protocole	Service	Description
8080	TCP	vsanvp	Utilisé pour le trafic de fournisseur de distributeur Virtual SAN.
9080	TCP	Service de filtre d'E/S	Utilisé par la fonctionnalité de stockage de filtres d'E/S

Tableau 3-6. Ports de pare-feu pour les services non visibles dans l'interface utilisateur par défaut

Port	Protocole	Service	Commentaire
5900-5964	TCP	Protocole RFB	Le protocole RFB est un protocole simple pour l'accès à distance aux interfaces utilisateur graphiques.
8889	TCP	Démon OpenWSMAN	Web Services Management (WS-Management est un standard ouvert DMTF pour la gestion des serveurs, des dispositifs, des applications et des services Web).

Comportement du pare-feu client NFS

L'ensemble de règles de pare-feu du client NFS ne se comporte pas comme les ensembles de règles de pare-feu ESXi. ESXi configure les paramètres du client NFS lorsque vous montez ou démontez une banque de données NFS. Le comportement dépend de la version de NFS.

Lorsque vous ajoutez, montez ou démontez une banque de données NFS, le comportement obtenu dépend de la version de NFS.

Comportement du pare-feu NFS v3

Lorsque vous ajoutez ou montez une banque de données NFS v3, ESXi vérifie l'état de l'ensemble de règles de pare-feu du client NFS (`nfsClient`).

- Si l'ensemble de règles `nfsClient` est désactivé, ESXi active l'ensemble de règles et désactive la stratégie « Autoriser toutes les adresses IP » en définissant l'indicateur `allowedAll` sur `FALSE`. L'adresse IP du serveur NFS est ajoutée à la liste des adresses IP sortantes autorisées.
- Si l'ensemble de règles `nfsClient` est activé, l'état de l'ensemble de règles et la stratégie d'adresse IP autorisée ne sont pas modifiés. L'adresse IP du serveur NFS est ajoutée à la liste des adresses IP sortantes autorisées.

Remarque Si vous activez manuellement l'ensemble de règles `nfsClient` ou configurez manuellement la stratégie Autoriser toutes les adresses IP, avant ou après avoir ajouté une banque de données NFS v3 dans le système, vos paramètres sont remplacés lorsque la dernière banque de données NFS v3 est démontée. L'ensemble de règles `nfsClient` est désactivé lorsque toutes les banques de données NFS v3 sont démontées.

Lorsque vous supprimez ou démontez une banque de données NFS v3, ESXi réalise l'une des actions suivantes.

- Si aucune des banques de données NFS v3 restantes n'est montée à partir du serveur de la banque de données que vous être en train de démonter, ESXi supprime l'adresse IP du serveur dans la liste des adresses IP sortantes.
- S'il ne reste aucune banque de données NFS v3 montée une fois l'opération de démontage terminée, ESXi désactive l'ensemble de règles de pare-feu `nfsClient`.

Comportement du pare-feu NFS v4.1

Lorsque vous montez la première banque de données NFS v4.1, ESXi active l'ensemble de règles `nfs41client` et définit son indicateur `allowedAll` sur TRUE. Cette action provoque l'ouverture du port 2049 pour toutes les adresses IP. Le démontage d'une banque de données NFS v4.1 n'a pas d'impact sur l'état du pare-feu. En d'autres termes, le port 2049 s'ouvre la première fois que vous montez une banque de données NFS v4.1 et reste ouvert jusqu'à ce que vous le fermiez explicitement.

Commandes de pare-feu ESXCLI d' ESXi

Si votre environnement inclut plusieurs hôtes ESXi, l'automatisation de la configuration de pare-feu à l'aide de commandes ESXCLI ou de vSphere Web Services SDK est recommandée.

Vous pouvez utiliser les commandes d'ESXi Shell ou de vSphere CLI pour configurer ESXi sur la ligne de commande afin d'automatiser la configuration du pare-feu. Reportez-vous à *Démarrage avec vSphere Command-Line Interfaces* pour une introduction et à *Concepts et exemples d'interfaces de ligne de commande vSphere* pour des exemples d'utilisation d'ESXCLI pour manipuler des pare-feu et des règles de pare-feu.

Tableau 3-7. Commandes du pare-feu

Commande	Description
`esxcli network firewall get`	Renvoie l'état activé ou désactivé du pare-feu et répertorie les actions par défaut.
`esxcli network firewall set --default-action`	Définir sur True pour transmettre les paquets par défaut. Définir sur False pour rejeter les paquets par défaut.
`esxcli network firewall set --enabled`	Activer ou désactiver le pare-feu d'ESXi.
`esxcli network firewall load`	Charger le module du pare-feu et les fichiers de configuration d'ensemble de règles.
`esxcli network firewall refresh`	Actualiser la configuration du pare-feu en lisant les fichiers d'ensemble de règles si le module du pare-feu est chargé.
`esxcli network firewall unload`	Détruire les filtres et décharger le module du pare-feu.
`esxcli network firewall ruleset list`	Répertorier les informations des ensembles de règles.
`esxcli network firewall ruleset set --allowed-all`	Définir sur True pour permettre l'accès à toutes les adresses IP. Définir sur False pour utiliser une liste d'adresses IP autorisées.
`esxcli network firewall ruleset set --enabled --ruleset-id=<string>`	Définir sur True pour activer l'ensemble de règles spécifié. Définir sur False pour le désactiver.
`esxcli network firewall ruleset allowedip list`	Répertorier les adresses IP autorisées de l'ensemble de règles spécifié.
`esxcli network firewall ruleset allowedip add`	Autoriser l'accès à l'ensemble de règles à partir de l'adresse IP ou de la plage d'adresses IP spécifiée.
`esxcli network firewall ruleset allowedip remove`	Supprimer l'accès à l'ensemble de règles à partir de l'adresse IP ou de la plage d'adresses IP spécifiée.
`esxcli network firewall ruleset rule list`	Lister les règles de chaque ensemble de règles du pare-feu.

Personnalisation des services ESXi à partir du profil de sécurité

Un hôte ESXi inclut plusieurs services s'exécutant par défaut. Vous pouvez désactiver les services depuis le profil de sécurité ou les activer si la stratégie de l'entreprise le nécessite.

« Utiliser vSphere Web Client pour activer l'accès à ESXi Shell », page 97 est un exemple de procédure d'activation d'un service.

Remarque L'activation de services affecte la sécurité de votre hôte. N'activez un service que si cela est strictement nécessaire.

Les services disponibles varient en fonction des VIB installés sur l'hôte ESXi. Vous ne pouvez pas ajouter de services sans installer un VIB. Certains produits VMware (par exemple, vSphere HA) installent des VIB sur des hôtes et rendent disponibles des services et les ports de pare-feu correspondants.

Dans une installation par défaut, vous pouvez modifier l'état des services suivants dans vSphere Web Client.

Tableau 3-8. Services ESXi du profil de sécurité

Service	Par défaut	Description
Interface utilisateur de la console directe	En cours d'exécution	Le service DCUI (Direct Console User Interface) vous permet d'interagir avec un hôte ESXi à partir de l'hôte de la console locale à l'aide de menus textuels.
ESXi Shell	Arrêté	ESXi Shell est disponible dans l'interface DCUI et inclut un ensemble de commandes intégralement prises en charge et un ensemble de commandes assurant le dépannage et la correction. Vous devez activer l'accès à ESXi Shell dans la console directe de chaque système. Vous pouvez activer l'accès à ESXi Shell ou accéder à ESXi Shell avec SSH.
SSH	Arrêté	Service client SSH de l'hôte qui permet les connexions à distance via SSH (Secure Shell).
Démon d'association basé sur la charge	En cours d'exécution	Association basée sur la charge.
Service Active Directory	Arrêté	Lorsque vous configurez ESXi pour Active Directory, ce service démarre.
Processus NTP	Arrêté	Démon NTP (Network Time Protocol).
Démon de carte à puce PC/SC	Arrêté	Lorsque vous activez l'hôte pour l'authentification par carte à puce, ce service démarre. Reportez-vous à « Configuration de l'authentification par carte à puce pour ESXi », page 94.
Serveur CIM	En cours d'exécution	Service pouvant être utilisé par les applications CIM (Common Information Model).
Serveur SNMP	Arrêté	Démon SNMP. Reportez-vous à *Surveillance et performances de vSphere* pour obtenir des informations sur la configuration de SNMP v1, v2 et v3.
Serveur Syslog	Arrêté	Démon Syslog. Vous pouvez activer syslog à partir des Paramètres système avancés de vSphere Web Client. Voir *Installation et configuration de vSphere*.

Tableau 3-8. Services ESXi du profil de sécurité (suite)

Service	Par défaut	Description
Agent VMware vCenter	En cours d'exécution	Agent vCenter Server. Autorise un système vCenter Server à se connecter à un hôte ESXi. Spécifiquement, vpxa est le conduit de communication au démon de l'hôte qui communique avec le noyau ESXi.
X.Org Server	Arrêté	X.Org Server. Cette fonctionnalité facultative est utilisée en interne pour les graphiques 3D des machines virtuelles.

Activer ou désactiver un service dans le profil de sécurité

Vous pouvez activer ou désactiver l'un des services répertoriés dans le profil de sécurité depuis vSphere Web Client.

Après l'installation, certains services s'exécutent par défaut, tandis que d'autres sont arrêtés. Dans certains cas, une configuration supplémentaire est nécessaire avant qu'un service devienne disponible dans l'interface utilisateur de vSphere Web Client. Par exemple, le service NTP permet d'obtenir des informations horaires précises, mais ce service fonctionne uniquement lorsque les ports requis sont ouverts dans le pare-feu.

Prérequis

Connectez-vous à vCenter Server avec vSphere Web Client.

Procédure

1 Accédez à un hôte dans l'inventaire vSphere Web Client, puis sélectionnez-le.

2 Cliquez sur **Configurer**.

3 Sous Système, sélectionnez **Profil de sécurité** et cliquez sur **Modifier**.

4 Accédez au service que vous souhaitez modifier.

5 Dans le volet Détails du service, sélectionnez **Démarrer**, **Arrêter** ou **Redémarrer** pour une modification ponctuelle de l'état de l'hôte ou faites votre choix dans le menu **Règle démarrage** pour modifier l'état de l'hôte lors des redémarrages.

   - **Démarrer automatiquement si ports ouverts, et arrêter quand tous ports fermés** : paramètre par défaut pour ces services. Si un port est ouvert, le client tente de contacter les ressources réseau du service. Si certains ports sont ouverts, mais que le port d'un service particulier est fermé, la tentative échoue. Lorsque le port sortant applicable est ouvert, le service termine son démarrage.
   - **Démarrer et arrêter avec hôte** : le service démarre peu après le démarrage de l'hôte, et s'arrête peu après l'arrêt de l'hôte. Plutôt semblable à l'option **Démarrer automatiquement si ports ouverts, et arrêter quand tous ports fermés**, cette option signifie que le service tente régulièrement d'effectuer sa tâche, telle que contacter le serveur NTP spécifié. Si le port a été fermé, mais est rouvert par la suite, le client commence à effectuer sa tâche peu après.

- **Démarrer et arrêter manuellement** : l'hôte conserve les paramètres de service déterminés par l'utilisateur, que les ports soient ouverts ou non. Lorsqu'un utilisateur démarre le service NTP, ce service reste en exécution tant que l'hôte est alimenté. Si le service est démarré et que l'hôte est mis hors tension, le service est arrêté dans le cadre du processus d'arrêt, mais dès que l'hôte est mis sous tension, le service redémarre et conserve l'état déterminé par l'utilisateur.

Remarque Ces paramètres s'appliquent uniquement aux paramètres de service qui sont configurés par le biais de vSphere Web Client ou aux applications créées avec vSphere Web Services SDK. Les configurations effectuées par d'autres moyens (par exemple, dans ESXi Shell ou avec les fichiers de configuration, ne sont pas modifiées par ces paramètres).

Mode verrouillage

Pour augmenter le niveau de sécurité des hôtes ESXi, vous pouvez les placer en mode de verrouillage. En mode de verrouillage, les opérations doivent être exécutées via vCenter Server par défaut.

vSphere 6.0 propose différents degrés de verrouillage par le biais de deux modes de verrouillage : normal et strict. La liste d'utilisateurs exceptionnels est une autre nouveauté de vSphere 6.0. Les utilisateurs exceptionnels ne perdent pas leurs privilèges lorsque l'hôte entre en mode de verrouillage. Utilisez la liste d'utilisateurs exceptionnels pour ajouter les comptes de solutions tierces et d'applications externes qui doivent accéder directement à l'hôte lorsque celui-ci est en mode de verrouillage. Reportez-vous à « Spécifier les utilisateurs exceptionnels du mode de verrouillage », page 82.

Mode verrouillage dans vSphere 6
(http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_lockdown_mode_vsphere)

Mode de verrouillage normal et mode de verrouillage strict

À partir de vSphere 6.0, vous pouvez sélectionner le mode de verrouillage normal ou le mode de verrouillage strict, ce qui offre différents degrés de verrouillage.

Mode de verrouillage normal

En mode de verrouillage normal, le service DCUI n'est pas interrompu. En cas de perte de connexion avec le système vCenter Server, si l'accès via vSphere Web Client n'est plus disponible, les comptes disposant de privilèges peuvent se connecter à l'interface utilisateur de la console directe de l'hôte ESXi et quitter le mode de verrouillage. Seuls les comptes suivants peuvent accéder à l'interface utilisateur de la console directe :

- Comptes répertoriés dans la liste des utilisateurs exceptionnels pour le mode de verrouillage qui disposent des privilèges d'administration sur l'hôte. La liste des utilisateurs exceptionnels est destinée aux comptes de service qui exécutent des tâches très spécifiques. L'ajout d'administrateurs ESXi à cette liste serait contraire à l'objectif du mode de verrouillage.

- Les utilisateurs définis dans l'option avancée DCUI.Access de l'hôte. Cette option sert d'accès de secours à l'interface utilisateur de la console directe en cas de perte de connexion avec vCenter Server. Ces utilisateurs n'ont pas besoin de disposer de privilèges d'administration sur l'hôte.

Mode de verrouillage strict

En mode de verrouillage strict (nouveau dans vSphere 6.0), le service DCUI est interrompu. En cas de perte de la connexion avec vCenter Server, si vSphere Web Client n'est plus disponible, l'hôte ESXi n'est plus disponible non plus, à moins que les services ESXi Shell et SSH soient activés et que des utilisateurs exceptionnels soient définis. Si vous ne pouvez pas rétablir la connexion avec le système vCenter Server, vous devez réinstaller l'hôte.

Mode de verrouillage et services ESXi Shell et SSH

Le mode de verrouillage strict interrompt le service DCUI. Toutefois, les services ESXi Shell et SSH sont indépendants du mode de verrouillage. Pour que le mode de verrouillage constitue une mesure de sécurité efficace, assurez-vous que les services ESXi Shell et SSH sont également désactivés. Ils sont désactivés par défaut.

Lorsqu'un hôte est en mode de verrouillage, les utilisateurs répertoriés dans la liste des utilisateurs exceptionnels peuvent accéder à l'hôte à partir de ESXi Shell et via SSH s'ils disposent du rôle Administrateur sur l'hôte. Cet accès reste possible en mode de verrouillage strict. Pour une sécurité maximale, laissez les services ESXi Shell et SSH désactivés.

Remarque La liste des utilisateurs exceptionnels est destinée aux comptes de service qui exécutent des tâches spécifiques, telles que les sauvegardes d'hôtes, pas aux administrateurs. L'ajout d'utilisateurs administrateurs à la liste des utilisateurs exceptionnels annule le mode de verrouillage.

Activation et désactivation du mode de verrouillage

Les utilisateurs disposant de privilèges peuvent activer le mode de verrouillage de plusieurs manières :

- En ajoutant un hôte à un système vCenter Server à l'aide de l'assistant Ajouter hôte.
- En utilisant vSphere Web Client. Reportez-vous à « Activation du mode verrouillage à l'aide de vSphere Web Client », page 79. Vous pouvez activer le mode de verrouillage normal et le mode de verrouillage strict dans vSphere Web Client.
- En utilisant l'interface utilisateur de la console directe (DCUI). Reportez-vous à « Activer ou désactiver le mode de verrouillage normal à partir de l'interface utilisateur de la console directe », page 80.

Les utilisateurs disposant de privilèges peuvent désactiver le mode de verrouillage dans vSphere Web Client. Dans cette interface, ils peuvent désactiver le mode de verrouillage normal, mais pas le mode de verrouillage strict.

Remarque Si vous activez ou désactivez le mode de verrouillage en utilisant l'interface utilisateur de la console directe, les autorisations des utilisateurs et des groupes sont ignorées sur l'hôte. Pour conserver ces autorisations, vous pouvez activer et désactiver le mode de verrouillage à l'aide de vSphere Web Client.

Comportement du mode de verrouillage

En mode de verrouillage, certains services sont désactivés et d'autres ne sont accessibles qu'à certains utilisateurs.

Services du mode de verrouillage pour différents utilisateurs

Lorsque l'hôte est en cours d'exécution, les services disponibles varient selon que le mode de verrouillage est activé et en fonction du type de mode de verrouillage.

- En mode de verrouillage strict et normal, les utilisateurs disposant de privilèges peuvent accéder à l'hôte via vCenter Server à l'aide de vSphere Web Client ou de vSphere Web Services SDK.
- Le comportement de l'interface de console directe du mode de verrouillage strict et différent de celui du mode de verrouillage normal.
  - En mode de verrouillage strict, le service d'interface utilisateur de la console directe est désactivé.
  - En mode de verrouillage normal, les comptes de la liste des utilisateurs exceptionnels qui disposent des privilèges d'administrateur et les utilisateurs spécifiés dans le paramètre système avancé DCUI.Access peuvent accéder à l'interface de console directe.
- Si ESXi Shell ou SSH est activé et que l'hôte est placé en mode de verrouillage strict ou normal, les comptes de la liste des utilisateurs exceptionnels qui disposent des privilèges d'administrateur peuvent utiliser ces services. ESXi Shell ou SSH est désactivé pour tous les autres utilisateurs. À partir de vSphere 6.0, les sessions ESXi ou SSH des utilisateurs qui ne disposent pas de privilèges d'administrateur sont terminées.

Tout accès est connecté à la fois pour le mode de verrouillage strict et normal.

Tableau 3-9. Comportement du mode de verrouillage

Service	Mode normal	Mode de verrouillage normal :	Mode verrouillage strict
API vSphere Web Services	Tous les utilisateurs, en fonction des autorisations	vCenter (vpxuser) Utilisateurs exceptionnels, en fonction des autorisations vCloud Director (vslauser, s'il est disponible)	vCenter (vpxuser) Utilisateurs exceptionnels, en fonction des autorisations vCloud Director (vslauser, s'il est disponible)
Fournisseurs CIM	Utilisateurs disposant des privilèges d'administrateur sur l'hôte	vCenter (vpxuser) Utilisateurs exceptionnels, en fonction des autorisations vCloud Director (vslauser, s'il est disponible)	vCenter (vpxuser) Utilisateurs exceptionnels, en fonction des autorisations vCloud Director (vslauser, s'il est disponible)
Interface utilisateur de la console directe (DCUI)	Utilisateurs disposant des privilèges d'administrateur sur l'hôte et utilisateurs de l'option avancée DCUI.Access	Utilisateurs définis dans l'option avancée DCUI.Access Utilisateurs exceptionnels disposant des privilèges d'administrateur sur l'hôte	Le service de l'interface DCUI est arrêté

Tableau 3-9. Comportement du mode de verrouillage (suite)

Service	Mode normal	Mode de verrouillage normal :	Mode verrouillage strict
ESXi Shell (s'il est activé)	Utilisateurs disposant des privilèges d'administrateur sur l'hôte	Utilisateurs définis dans l'option avancée DCUI.Access Utilisateurs exceptionnels disposant des privilèges d'administrateur sur l'hôte	Utilisateurs définis dans l'option avancée DCUI.Access Utilisateurs exceptionnels disposant des privilèges d'administrateur sur l'hôte
SSH (s'il est activé)	Utilisateurs disposant des privilèges d'administrateur sur l'hôte	Utilisateurs définis dans l'option avancée DCUI.Access Utilisateurs exceptionnels disposant des privilèges d'administrateur sur l'hôte	Utilisateurs définis dans l'option avancée DCUI.Access Utilisateurs exceptionnels disposant des privilèges d'administrateur sur l'hôte

Utilisateurs connectés à ESXi Shell lorsque le mode de verrouillage est activé

Si des utilisateurs sont connectés à ESXi Shell ou accèdent à l'hôte via SSH avant d'activer le mode de verrouillage, les utilisateurs qui se trouvent sur la liste des utilisateurs exceptionnels et qui disposent des privilèges d'administrateur sur l'hôte restent connectés. À partir de vSphere 6.0, la session est terminée pour tous les autres utilisateurs. Ce comportement s'applique à la fois au mode de verrouillage normal et strict.

Activation du mode verrouillage à l'aide de vSphere Web Client

Vous pouvez activer le mode de verrouillage afin d'imposer l'apport des modifications de configuration via vCenter Server. vSphere 6.0 et versions ultérieures prennent en charge le mode de verrouillage normal et strict.

Pour interdire complètement tout accès direct à un hôte, vous pouvez sélectionner le mode de verrouillage strict. Le mode de verrouillage strict empêche d'accéder à un hôte si vCenter Server n'est pas disponible et que SSH et ESXi Shell sont désactivés. Reportez-vous à « Comportement du mode de verrouillage », page 78.

Procédure

1 Accédez à l'hôte dans l'inventaire de vSphere Web Client.

2 Cliquez sur **Configurer**.

3 Dans Système, sélectionnez **Profil de sécurité**.

4 Dans le panneau mode verrouillage, cliquez sur **Modifier**.

5 Cliquez sur **Mode verrouillage** et sélectionnez l'une des options du mode de verrouillage.

Option	Description
Normale	Vous pouvez accéder à l'hôte via vCenter Server. Seuls les utilisateurs qui se trouvent dans la liste des utilisateurs exceptionnels et qui disposent des privilèges d'administrateur peuvent se connecter à l'interface utilisateur de la console directe. Si SSH ou ESXi Shell sont activés, il peut être possible d'y accéder.
Strict	Vous ne pouvez accéder à l'hôte que via vCenter Server. Si SSH ou ESXi Shell sont activés, les sessions des comptes de l'option avancée DCUI.Access et des comptes d'utilisateurs exceptionnels disposant de privilèges d'administrateur restent activées. Toutes les autres sessions sont terminées.

6 Cliquez sur **OK**.

Désactiver le mode de verrouillage à l'aide de vSphere Web Client

Désactivez le mode de verrouillage pour permettre des modifications de configuration à partir de connexions directes à l'hôte ESXi. Lorsque le mode de verrouillage est activé, la sécurité de l'environnement est accrue.

Dans vSphere 6.0, vous pouvez désactiver le mode de verrouillage comme suit :

Dans vSphere Web Client Les utilisateurs peuvent désactiver à la fois le mode de verrouillage normal et strict dans vSphere Web Client.

Dans l'interface utilisateur de la console directe Les utilisateurs qui peuvent accéder à l'interface utilisateur de la console directe sur l'hôte ESXi peuvent désactiver le mode de verrouillage normal. En mode de verrouillage strict, le service d'interface de console directe est arrêté.

Procédure

1 Accédez à l'hôte dans l'inventaire de vSphere Web Client.

2 Cliquez sur **Configurer**.

3 Dans Système, sélectionnez **Profil de sécurité**.

4 Dans le panneau mode verrouillage, cliquez sur **Modifier**.

5 Cliquez sur **Mode verrouillage** et sélectionnez **Aucun** pour désactiver le mode de verrouillage.

Le système quitte le mode de verrouillage, vCenter Server affiche une alarme et une entrée est ajoutée au journal d'audit.

Activer ou désactiver le mode de verrouillage normal à partir de l'interface utilisateur de la console directe

Vous pouvez activer et désactiver le mode de verrouillage normal dans l'interface utilisateur de la console directe (DCUI). Vous ne pouvez activer et désactiver le mode de verrouillage strict que dans vSphere Web Client.

Lorsque l'hôte est en mode de verrouillage normal, les comptes suivants peuvent accéder à l'interface utilisateur de la console directe :

- Les comptes de la liste des utilisateurs exceptionnels qui disposent des privilèges d'administrateur sur l'hôte. La liste des utilisateurs exceptionnels est destinée aux comptes de service tels qu'un agent de sauvegarde.
- Les utilisateurs définis dans l'option avancée DCUI.Access de l'hôte. Cette option peut être utilisée pour activer l'accès en cas de défaillance irrémédiable.

Pour ESXi 6.0 et versions ultérieures, les autorisations des utilisateurs sont conservées lorsque vous activez le mode de verrouillage et restaurées lorsque vous désactivez ce mode dans l'interface de console directe.

Remarque Si vous mettez à niveau un hôte en mode de verrouillage vers ESXi 6.0 sans quitter le mode de verrouillage, puis que vous quittez ce mode après la mise à niveau, toutes les autorisations définies avant que l'hôte n'entre en mode de verrouillage sont perdues. Le système attribue le rôle d'administrateur à tous les utilisateurs qui se trouvent dans l'option avancée DCUI.Access afin d'assurer l'accès à l'hôte.

Pour conserver les autorisations, désactivez le mode de verrouillage de l'hôte dans vSphere Web Client avant la mise à niveau.

Procédure

1 Dans l'interface utilisateur de la console directe de l'hôte, appuyez sur F2 et ouvrez une session.

2 Faites défiler jusqu'au paramètre **Configurer le mode verrouillage** et appuyez sur Entrée pour modifier le paramètre actuel.

3 Appuyez sur Échap jusqu'à ce que vous reveniez au menu principal de l'interface utilisateur de console directe.

Spécification des comptes disposant de privilèges d'accès en mode de verrouillage

Vous pouvez spécifier les comptes de service qui peuvent accéder à l'hôte ESXi directement en les ajoutant à la liste des utilisateurs exceptionnels. Vous pouvez spécifier un utilisateur qui peut accéder à l'hôte ESXi en cas de défaillance irrémédiable de vCenter Server.

Les actions par défaut que peuvent effectuer les différents comptes lorsque le mode de verrouillage est activé et le mode de modification du comportement par défaut dépendent de la version de l'environnement vSphere.

- Dans les versions de vSphere antérieures à vSphere 5.1, seul l'utilisateur racine peut se connecter à l'interface utilisateur de la console directe sur un hôte ESXi en mode de verrouillage.
- Dans vSphere 5.1 et versions ultérieures, vous pouvez ajouter un utilisateur au paramètre système avancé DCUI.Access pour chaque hôte. Cette option est conçue pour répondre aux défaillances irrémédiables de vCenter Server et le mot de passe de l'utilisateur disposant de cet accès est habituellement verrouillé dans un coffre-fort. Un utilisateur de la liste DCUI.Access n'a pas besoin de disposer de tous les privilèges administratifs sur l'hôte.
- Dans vSphere 6.0 et versions ultérieures, le paramètre système avancé DCUI.Access est toujours pris en charge. En outre, vSphere 6.0 et versions ultérieures prennent en charge une liste des utilisateurs exceptionnels destinée aux comptes de service qui doivent se connecter directement à l'hôte. Les comptes d'administrateur disposant des privilèges d'administrateur, qui se trouvent dans la liste des utilisateurs exceptionnels, peuvent se connecter à ESXi Shell. En outre, ces utilisateur peuvent se connecter à l'interface DCUI d'un hôte en mode de verrouillage normal et quitter ce même mode.

  Spécifiez les utilisateurs exceptionnels dans vSphere Web Client

  Remarque Les utilisateurs exceptionnels sont des utilisateurs locaux d'un hôte ou des utilisateurs Active Directory disposant de privilèges définis localement pour l'hôte ESXi. Les utilisateurs qui sont membres d'un groupe Active Directory perdre leurs autorisations lorsque l'hôte est en mode de verrouillage.

Option avancée Ajouter des utilisateurs à DCUI.Access

L'option avancée DCUI.Access a pour objectif principal de vous permettre de quitter le mode de verrouillage en cas de défaillance irrémédiable, lorsque vous ne pouvez pas accéder à l'hôte à partir de vCenter Server. Vous ajoutez des utilisateurs à la liste en modifiant les paramètres avancés de l'hôte à partir de vSphere Web Client.

Remarque Les utilisateurs de la liste DCUI.Access peuvent modifier les paramètres du mode de verrouillage, quels que soient leurs privilèges. Cela peut avoir un impact sur la sécurité de votre hôte. Pour les comptes de services qui ont besoin d'un accès direct à l'hôte, pensez plutôt à ajouter des utilisateurs à la liste des utilisateurs exceptionnels. Les utilisateurs exceptionnels peuvent uniquement exécuter les tâches pour lesquelles ils ont des privilèges. Reportez-vous à « Spécifier les utilisateurs exceptionnels du mode de verrouillage », page 82.

Procédure

1 Accédez à l'hôte dans le navigateur d'objets de vSphere Web Client.

2 Cliquez sur **Configurer**.

3 Dans la section Système, cliquez sur **Paramètres système avancés**, puis sur **Modifier**.

4 Appliquez le filtre à l'interface DCUI.

5 Dans la zone de texte **DCUI.Access**, entrez les noms d'utilisateur, séparés par des virgules.

   L'utilisateur racine est inclus par défaut. Pensez à supprimer la racine de la liste DCUI.Access et à spécifier un compte nommé pour un meilleur contrôle.

6 Cliquez sur **OK**.

Spécifier les utilisateurs exceptionnels du mode de verrouillage

Dans vSphere 6.0 et versions ultérieures, vous pouvez ajouter des utilisateurs à la liste des utilisateurs exceptionnels dans vSphere Web Client. Ces utilisateurs ne perdent pas leurs autorisations lorsque l'hôte entre en mode de verrouillage. Il est logique d'ajouter des comptes de services tels qu'un agent de sauvegarde à la liste des utilisateurs exceptionnels.

Les utilisateurs exceptionnels ne perdent pas leurs privilèges lorsque l'hôte entre en mode de verrouillage. Habituellement, ces comptes représentent des solutions tierces et des applications externes qui doivent continuer à fonctionner en mode de verrouillage.

Remarque La liste des utilisateurs exceptionnels est destinée aux comptes de service qui exécutent des tâches très spécifiques, pas aux administrateurs. L'ajout d'utilisateurs administrateurs à la liste des utilisateurs exceptionnels annule le mode de verrouillage.

Les utilisateurs exceptionnels sont des utilisateurs locaux d'un hôte ou des utilisateurs Active Directory disposant de privilèges définis localement pour l'hôte ESXi. Ils ne sont ni membres d'un groupe Active Directory ni utilisateurs de vCenter Server. Ces utilisateurs sont autorisés à effectuer des opérations sur l'hôte en fonction de leurs privilèges. Par exemple, cela signifie que l'utilisateur en lecture seule ne peut pas désactiver le mode de verrouillage sur un hôte.

Procédure

1 Accédez à l'hôte dans l'inventaire de vSphere Web Client.

2 Cliquez sur **Configurer**.

3 Dans Système, sélectionnez **Profil de sécurité**.

4 Dans le panneau mode verrouillage, cliquez sur **Modifier**.

5 Cliquez sur **Utilisateurs exceptionnels** et sur l'icône représentant le signe plus pour ajouter des utilisateurs exceptionnels.

Vérifier les niveaux d'acceptation des hôtes et des fichiers VIB

Le niveau d'acceptation d'un VIB dépend du montant de certification de ce VIB. Le niveau d'acceptation de l'hôte dépend du niveau du VIB inférieur. Vous pouvez modifier le niveau d'acceptation de l'hôte si vous souhaitez autoriser les VIB de niveau inférieur. Vous pouvez supprimer les VIB CommunitySupported pour modifier le niveau d'acceptation de l'hôte.

Les VIB sont des modules logiciels qui incluent une signature de VMware ou d'un partenaire VMware. Pour protéger l'intégrité de l'hôte ESXi, n'autorisez pas les utilisateurs à installer des VIB non signés (communautaires). Un VIB non signé contient un code qui n'est ni certifié ni approuvé ni pris en charge par VMware ou ses partenaires. Les VIB communautaires n'ont pas de signature numérique.

Le niveau d'acceptation de l'hôte doit être le même ou moins restrictif que celui d'un VIB que vous souhaitez ajouter à l'hôte. Par exemple, si le niveau d'acceptation de l'hôte est VMwareAccepted, vous ne pouvez pas installer les VIB au niveau PartnerSupported. Vous pouvez utiliser des commandes ESXCLI pour définir le niveau de l'acceptation d'un hôte. Pour protéger la sécurité et l'intégrité de vos hôtes ESXi, ne permettez pas l'installation de VIB non signés (CommunitySupported) sur des hôtes dans des systèmes de production.

Le niveau d'acceptation d'un hôte ESXi s'affiche dans le **Profil de sécurité** dans vSphere Web Client.

Les niveaux d'acceptation suivants sont pris en charge.

VMwareCertified	Le niveau d'acceptation VMwareCertified a les exigences les plus contraignantes. Les VIB avec ce niveau sont soumis à des tests minutieux équivalents aux tests d'assurance qualité réalisés en interne de VMware pour la même technologie. Actuellement, seuls les pilotes IOVP sont publiés à ce niveau. VMware prend en charge les appels d'assistance pour les VIB avec ce niveau d'acceptation.
VMwareAccepted	Les VIB avec ce niveau d'acceptation sont soumis à des tests de vérification minutieux, mais ces tests ne testent pas entièrement chaque fonction du logiciel. Le partenaire exécute les tests et VMware vérifie le résultat. Actuellement, les fournisseurs CIM et les plug-ins PSA font partie des VIB publiés à ce niveau. VMware dirige les appels d'assistance pour les VIB avec ce niveau d'acceptation vers l'organisation d'assistance du partenaire.
PartnerSupported	Les VIB avec le niveau d'acceptation PartnerSupported sont publiés par un partenaire en qui VMware a confiance. Le partenaire effectue tous les tests. VMware ne vérifie pas les résultats. Ce niveau est utilisé pour une technologie nouvelle ou non courante que des partenaires souhaitent activer pour les systèmes VMware. Actuellement, les technologies VIB de pilotes telles que Infiniband, ATAoE et SSD sont à ce niveau avec des pilotes de matériel non standard. VMware dirige les appels d'assistance pour les VIB avec ce niveau d'acceptation vers l'organisation d'assistance du partenaire.
CommunitySupported	Le niveau d'acceptation CommunitySupported est destiné aux VIB créés par des individus ou des entreprises en dehors des programmes de partenariat de VMware. Les VIB à ce niveau d'acceptation ne sont soumis à aucun programme de test approuvé par VMware et ne sont pas pris en charge par l'assistance technique de VMware ou un partenaire de VMware.

Procédure

1 Connectez-vous à chaque hôte ESXi et vérifiez que le niveau d'acceptation est défini sur VMwareCertified, VMwareAccepted ou PartnerSupported en exécutant la commande suivante.

```
esxcli software acceptance get
```

2 Si le niveau d'acceptation de l'hôte est CommunitySupported, déterminez si un ou plusieurs VIB sont au niveau CommunitySupported en exécutant les commandes suivantes.

```
esxcli software vib list
esxcli software vib get –n vibname
```

3 Supprimez les VIB CommunitySupported en exécutant la commande suivante.

```
esxcli software vib remove ––vibname vib
```

4 Changez le niveau d'acceptation de l'hôte en exécutant la commande suivante.

```
esxcli software acceptance set ––level acceptance_level
```

Attribution de privilèges pour les hôtes ESXi

Les privilèges sont généralement octroyés aux utilisateurs par attribution d'autorisations aux objets hôtes ESXi gérés par un système vCenter Server. Si vous utilisez un hôte ESXi autonome, vous pouvez attribuer les privilèges directement.

Attribution d'autorisations aux hôtes ESXi gérés par vCenter Server

Si votre hôte ESXi est géré par vCenter Server, effectuez les tâches de gestion à l'aide de vSphere Web Client.

Vous pouvez sélectionner l'objet hôte ESXi dans la hiérarchie d'objets de vCenter Server et attribuer le rôle d'administrateur à un nombre limité d'utilisateurs susceptibles d'effectuer la gestion directe sur l'hôte ESXi. Reportez-vous à « Utilisation des rôles pour assigner des privilèges », page 32.

Il est recommandé de créer au moins un compte d'utilisateur nommé et de lui attribuer des privilèges d'administration complets sur l'hôte, puis de l'utiliser à la place du compte racine. Définissez un mot de passe avec un niveau de complexité élevé pour le compte racine et limitez l'utilisation de ce compte. Ne supprimez pas le compte racine.

Attribution d'autorisations aux hôtes ESXi autonomes

Si votre environnement ne comprend pas de système vCenter Server, les utilisateurs suivants sont prédéfinis.

- utilisateur racine. Reportez-vous à « Privilèges de l'utilisateur racine », page 85.
- vpxuser. Reportez-vous à « Privilèges vpxuser », page 85.
- utilisateur dcui. Reportez-vous à « Privilèges de l'utilisateur dcui », page 85.

Dans l'onglet Gestion de VMware Host Client, vous pouvez ajouter des utilisateurs locaux et définir des rôles personnalisés. Consultez la documentation de *Gestion individuelle des hôtes vSphere - VMware Host Client*.

Les rôles suivants sont prédéfinis :

Lecture seule	Permet à un utilisateur d'afficher les objets associés à l'hôte ESXi, mais pas de les modifier.
Administrateur	Rôle d'administrateur.
Aucun accès	Aucun accès. Ce rôle est le rôle par défaut. Vous pouvez remplacer le rôle par défaut.

Vous pouvez gérer les utilisateurs et les groupes locaux et ajouter des rôles personnalisés locaux à un hôte ESXi à l'aide d'une instance de VMware Host Client directement connectée à l'hôte ESXi. Consultez la documentation de *Gestion individuelle des hôtes vSphere - VMware Host Client*.

À partir de vSphere 6.0, vous pouvez gérer les comptes d'utilisateurs locaux ESXi à l'aide des commandes de gestion de compte ESXCLI. Vous pouvez définir ou supprimer des autorisations sur les comptes Active Directory (utilisateurs et groupes) et sur les comptes locaux ESXi (utilisateurs uniquement) à l'aide des commandes de gestion des autorisations ESXCLI.

Remarque Si vous définissez un utilisateur pour l'hôte ESXi en le connectant directement à l'hôte et qu'il existe un utilisateur de même nom dans vCenter Server, ces deux utilisateurs sont distincts. Si vous attribuez un rôle à l'utilisateur ESXi, il n'est pas attribué à l'utilisateur vCenter Server.

Privilèges de l'utilisateur racine

Par défaut, chaque hôte ESXi dispose d'un compte d'utilisateur racine unique ayant le rôle Administrateur. Ce compte d'utilisateur racine peut être utilisé pour l'administration locale et pour connecter l'hôte à vCenter Server.

Ce compte racine commun peut faciliter l'accès à un hôte ESXi car le nom est déjà connu. Un compte racine commun rend également plus difficile la mise en correspondance des actions avec les utilisateurs.

Pour optimiser l'audit, créez des comptes individuels avec des privilèges d'administrateur. Définissez un mot de passe très complexe pour le compte racine et limitez l'utilisation de ce compte (par exemple, pour une utilisation lors de l'ajout d'un hôte à vCenter Server). Ne supprimez pas le compte racine.

Il convient de s'assurer que tout compte disposant du rôle Administrateur sur un hôte ESXi est attribué à un utilisateur spécifique ayant un compte nommé. Utilisez les fonctionnalités Active Directory d'ESXi, qui vous permettent de gérer les informations d'identification Active Directory.

Important Si vous supprimez les privilèges d'accès de l'utilisateur racine, vous devez d'abord créer une autre autorisation au niveau de la racine ayant un autre utilisateur affecté au rôle d'administrateur.

Privilèges vpxuser

vCenter Server utilise les privilèges vpxuser pour gérer les activités de l'hôte.

vCenter Server possède des privilèges d'administrateur sur l'hôte qu'il gère. Par exemple, vCenter Server peut transférer des machines virtuelles vers/depuis des hôtes et effectuer les changements de configuration requis pour prendre en charge des machines virtuelles.

L'administrateur vCenter Server peut exécuter sur l'hôte la majorité des tâches de l'utilisateur racine, mais aussi programmer des tâches, utiliser des modèles, etc. Cependant, l'administrateur vCenter Server ne peut pas directement créer, supprimer ou modifier des utilisateurs et groupes locaux pour des hôtes. Ces tâches peuvent uniquement être exécutées par un utilisateur disposant des autorisations administrateur directement sur chaque hôte.

Remarque Vous ne pouvez pas gérer vpxuser via Active Directory.

Avertissement Ne modifiez vpxuser en aucune façon. Ne modifiez pas son mot de passe. Ne modifiez pas ses autorisations. Dans le cas contraire, vous risquez d'avoir des difficultés à utiliser des hôtes via vCenter Server.

Privilèges de l'utilisateur dcui

L'utilisateur dcui s'exécute sur des hôtes et dispose des droits d'Administrateur. L'objectif principal de cet utilisateur est de configurer des hôtes pour le mode verrouillage à partir de l'interface utilisateur de console directe (DCUI).

Cet utilisateur agit en tant qu'agent pour la console directe et ne peut pas être modifié ou utilisé par des utilisateurs interactifs.

Utilisation d'Active Directory pour gérer des utilisateurs ESXi

Vous pouvez configurer l'hôte ESXi afin qu'il utilise un service d'annuaire tel qu'Active Directory pour gérer les utilisateurs.

La création de comptes utilisateurs locaux sur chaque hôte pose des difficultés de synchronisation du nom et du mot de passe des comptes parmi plusieurs hôtes. Intégrez les hôtes ESXi à un domaine Active Directory pour éliminer la nécessité de créer et de maintenir des comptes utilisateurs locaux. L'utilisation d'Active Directory pour l'authentification des utilisateurs simplifie la configuration de l'hôte ESXi et réduit le risque de problèmes de configuration qui pourraient entraîner des accès non autorisés.

Lorsque vous utilisez Active Directory, les utilisateurs entrent les informations d'identification Active Directory et le nom de domaine du serveur Active Directory lorsqu'ils ajoutent un hôte à un domaine.

Configurer un hôte pour utiliser Active Directory

Vous pouvez configurer un hôte pour utiliser un service d'annuaire comme Active Directory afin de gérer les groupes de travail et les utilisateurs.

Lorsque vous ajoutez un hôte ESXi à Active Directory, le groupe DOMAIN **ESX Admins** obtient un accès administratif complet à l'hôte s'il existe. Si vous ne voulez pas rendre disponible l'accès administratif complet, consultez l'article 1025569 de la base de connaissances VMware pour une solution.

Si un hôte est provisionné avec Auto Deploy, les informations d'identification Active Directory ne peuvent pas être stockées sur les hôtes. Vous pouvez utiliser vSphere Authentication Proxy pour joindre l'hôte à un domaine Active Directory. Comme une chaîne d'approbation existe entre vSphere Authentication Proxy et l'hôte, Authentication Proxy peut joindre l'hôte au domaine Active Directory. Reportez-vous à « Utiliser vSphere Authentication Proxy », page 88.

Remarque Lorsque vous définissez des paramètres de comptes d'utilisateurs dans Active Directory, vous pouvez limiter les ordinateurs auxquels un utilisateur peut se connecter en fonction du nom de ces ordinateurs. Par défaut, aucune restriction équivalente n'est définie pour un compte utilisateur. Si vous définissez cette limitation, les demandes Bind LDAP pour le compte d'utilisateur échouent avec le message `LDAP binding not successful`, même si la demande provient d'un ordinateur référencé. Vous pouvez éviter ce problème en ajoutant le nom netBIOS du serveur Active Directory à la liste des ordinateurs auxquels le compte utilisateur peut se connecter.

Prérequis

- Vérifiez que vous disposez d'un domaine Active Directory. Reportez-vous à la documentation de votre serveur d'annuaire.
- Assurez-vous que le nom d'hôte d'ESXi est complet et inclut le nom de domaine de la forêt Active Directory.

  fully qualified domain name = host_name.domain_name

Procédure

1 Synchronisez le temps entre ESXi et le système de service d'annuaire en utilisant NTP.

  Consultez la base des connaissances « Synchroniser les horloges ESXi avec un serveur de temps réseau », page 186 ou la base des connaissances VMware pour plus d'informations sur la synchronisation de l'heure ESXi avec un contrôleur de domaine Microsoft.

2 Assurez-vous que les serveurs DNS que vous avez configurés pour l'hôte peuvent résoudre les noms d'hôtes des contrôleurs Active Directory.

  a Accédez à l'hôte dans le navigateur d'objets de vSphere Web Client.

  b Cliquez sur **Configurer**.

c Sous Mise en réseau, cliquez sur **Configuration TCP/IP**.

d Sous Pile TCP/IP : par défaut, cliquez sur **DNS** et vérifiez que le nom d'hôte et les informations relatives au serveur DNS de l'hôte sont correctes.

Suivant

Utilisez vSphere Web Client pour rejoindre un domaine de service d'annuaire. Reportez-vous à « Ajouter un hôte à un domaine de service d'annuaire », page 87. Pour les hôtes provisionnés avec Auto Deploy, configurez vSphere Authentication Proxy. Reportez-vous à « Utiliser vSphere Authentication Proxy », page 88.

Ajouter un hôte à un domaine de service d'annuaire

Pour que votre hôte utilise un service d'annuaire, vous devez joindre l'hôte au domaine du service d'annuaire.

Vous pouvez entrer le nom de domaine de l'une des deux façons suivantes :

- **`name.tld`** (par exemple, **`domain.com`**): Le compte est créé sous le récipient par défaut.
- **`name.tld/container/path`** (par exemple, **`domain.com/OU1/OU2`**) : Le compte est créé sous une unité d'organisation (OU) précise.

Pour utiliser le service vSphere Authentication Proxy, consultez« Utiliser vSphere Authentication Proxy », page 88.

Procédure

1 Accédez à l'hôte dans l'inventaire de vSphere Web Client.

2 Cliquez sur **Configurer**.

3 Sous Système, sélectionnez **Services d'authentification**.

4 Cliquez sur **Joindre le domaine**.

5 Entrez un domaine.

Utilisez le format **`name.tld`** ou **`name.tld/container/path`**.

6 Entrez le nom d'utilisateur et le mot de passe d'un utilisateur service d'annuaire autorisé à lier l'hôte au domaine, puis cliquez sur **OK**.

7 (Facultatif) Si vous avez l'intention d'utiliser un proxy d'authentication, entrez l'adresse IP du serveur proxy.

8 Cliquez sur **OK** pour fermer la boîte de dialogue Configuration des services d'annuaire.

Afficher les paramètres du service d'annuaire

Vous pouvez afficher le type de serveur d'annuaire, le cas échéant, que l'hôte utilise pour authentifier les utilisateurs et les paramètres du serveur d'annuaire.

Procédure

1 Accédez à l'hôte dans l'inventaire de vSphere Web Client.

2 Cliquez sur **Configurer**.

3 Sous Système, sélectionnez **Services d'authentification**.

La page Services d'authentification affiche le service d'annuaire et les paramètres du domaine.

Utiliser vSphere Authentication Proxy

Vous pouvez ajouter des hôtes ESXi à un domaine Active Directory en utilisant vSphere Authentication Proxy plutôt que d'ajouter les hôtes explicitement au domaine Active Directory.

Vous devez simplement configurer l'hôte de sorte qu'il connaisse le nom de domaine du serveur Active Directory et l'adresse IP de vSphere Authentication Proxy. Lorsque vSphere Authentication Proxy est activé, il ajoute automatiquement les hôtes qui sont en cours de provisionnement avec Auto Deploy au domaine Active Directory. Vous pouvez également utiliser vSphere Authentication Proxy avec des hôtes qui ne sont pas provisionnés en utilisant Auto Deploy.

Auto Deploy

Si vous provisionnez des hôtes avec Auto Deploy, vous pouvez configurer un hôte de référence qui pointe vers Authentication Proxy. Vous pouvez configurer une règle qui applique le profil de l'hôte de référence à un hôte ESXi qui est provisionné avec Auto Deploy. vSphere Authentication Proxy stocke les adresses IP de tous les hôtes qu'Auto Deploy provisionne à l'aide de PXE dans sa liste de contrôle d'accès. Lorsque l'hôte démarre, il contacte vSphere Authentication Proxy, et vSphere Authentication Proxy joint ces hôtes, qui se trouvent déjà dans sa liste de contrôle d'accès, sur le domaine Active Directory.

Même si vous utilisez vSphere Authentication Proxy dans un environnement utilisant des certificats provisionnés par VMCA ou des certificats tiers, le processus se déroule de manière transparente si vous suivez les instructions d'utilisation des certificats personnalisés avec Auto Deploy.

Reportez-vous à « Utiliser des certificats personnalisés avec Auto Deploy », page 65.

Autres hôtes ESXi

Vous pouvez configurer d'autres hôtes pour qu'ils utilisent vSphere Authentication Proxy si vous souhaitez que l'hôte puisse joindre le domaine sans utiliser les informations d'identification d'Active Directory. Cela signifie que vous n'avez pas besoin de transmettre les informations d'identification d'Active Directory à l'hôte, et que vous n'enregistrez pas les informations d'identification d'Active Directory dans le profil hôte.

Dans ce cas, vous ajoutez l'adresse IP de l'hôte à la liste de contrôle d'accès de vSphere Authentication Proxy, et vSphere Authentication Proxy autorise l'hôte basé sur son adresse IP par défaut. Vous pouvez activer l'autentification client de sorte que vSphere Authentication Proxy vérifie le certificat de l'hôte.

Remarque Vous ne pouvez pas utiliser vSphere Authentication Proxy dans un environnement qui prend uniquement en charge IPv6.

Activer vSphere Authentication Proxy

Le service vSphere Authentication Proxy est disponible sur chaque système vCenter Server. Par défaut, ce service ne s'exécute pas. Si vous souhaitez utiliser vSphere Authentication Proxy dans votre environnement, vous pouvez démarrer ce service depuis vSphere Web Client ou depuis la ligne de commande.

Le service vSphere Authentication Proxy se lie à une adresse IPv4 pour communiquer avec vCenter Server et ne prend pas en charge IPv6. L'instance vCenter Server peut être sur une machine hôte dans un environnement réseau exclusivement IPv4 ou mixte, IPv4/IPv6. Cependant, lorsque vous spécifiez l'adresse de vSphere Authentication Proxy dans vSphere Web Client, vous devez spécifier une adresse IPv4.

Prérequis

Vous devez utiliser vCenter Server 6.5 ou une version plus récente. Dans les versions précédentes de vSphere, vSphere Authentication Proxy est installé séparément. Reportez-vous à la documentation de la version précédente du produit pour connaître les instructions.

Procédure

1 Connectez-vous à un système vCenter Server avec vSphere Web Client.

2 Cliquez sur **Administration**, puis sur **Configuration système** sous **Déploiement**.

3 Cliquez sur **Services**, puis sur le service **VMware vSphere Authentication Proxy**.

4 Cliquez sur l'icône verte **Démarrer le service** de la barre de menus, en haut de la fenêtre.

5 (Facultatif) Une fois le service démarré, cliquez sur **Actions > Modifier le type de démarrage** et cliquez sur **Automatique** pour démarrer automatiquement le service par la suite.

Vous pouvez désormais définir le domaine vSphere Authentication Proxy. Ensuite, vSphere Authentication Proxy traite tous les hôtes qui sont provisionnés avec Auto Deploy et vous pouvez ajouter explicitement des hôtes à vSphere Authentication Proxy.

Ajouter un domaine à vSphere Authentication Proxy avec vSphere Web Client

Vous pouvez ajouter un domaine vSphere Authentication Proxy depuis vSphere Web Client ou en exécutant la commande `camconfig`.

Vous pouvez ajouter un domaine à vSphere Authentication Proxy uniquement après avoir activé le proxy. Dès que vous avez ajouté le domaine, vSphere Authentication Proxy ajoute à celui-ci tous les hôtes que vous provisionnez avec Auto Deploy. Pour les autres hôtes, vous pouvez également utiliser vSphere Authentication Proxy si vous ne souhaitez pas leur accorder des privilèges de domaine.

Procédure

1 Connectez-vous à un système vCenter Server avec vSphere Web Client.

2 Cliquez sur **Administration**, puis sur **Configuration système** sous **Déploiement**.

3 Cliquez sur **Services**, cliquez sur le service **VMware vSphere Authentication Proxy**, puis cliquez sur **Modifier**.

4 Entrez le nom du domaine dans lequel le service vSphere Authentication Proxy ajoutera les hôtes, ainsi que le nom d'un utilisateur qui dispose de privilèges Active Directory permettant d'ajouter des hôtes dans ce domaine.

   Les autres champs de cette boîte de dialogue sont donnés uniquement à titre indicatif.

5 Cliquez sur l'icône en forme de points de suspension pour ajouter et confirmer le mot de passe de l'utilisateur, puis cliquez sur **OK**.

Ajouter un domaine à vSphere Authentication Proxy avec la commande camconfig

Vous pouvez ajouter un domaine au serveur d'authentification vSphere depuis vSphere Web Client ou en exécutant la commande `camconfig`.

Vous pouvez ajouter un domaine à vSphere Authentication Proxy uniquement après avoir activé le proxy. Dès que vous avez ajouté le domaine, vSphere Authentication Proxy ajoute à celui-ci tous les hôtes que vous provisionnez avec Auto Deploy. Pour les autres hôtes, vous pouvez également utiliser vSphere Authentication Proxy si vous ne souhaitez pas leur accorder des privilèges de domaine.

Procédure

1 Connectez-vous à vCenter Server Appliance ou à la machine Windows sur laquelle vCenter Server est installé en tant qu'utilisateur avec des privilèges d'administrateur.

2 Exécutez la commande pour activer l'accès à l'interpréteur de commandes de dépistage.

```
shell
```

3 Accédez au répertoire dans lequel le script **camconfig** se trouve.

SE	Emplacement
Dispositif vCenter Server	`/usr/lib/vmware-vmcam/bin/`
vCenter Server sous Windows	`C:\Program Files\VMware\CIS\vmcamd\`

4 Exécutez la commande suivante pour ajouter le domaine et les informations d'identification Active Directory à la configuration du serveur proxy d'authentification.

```
camconfig add-domain -d domain -u user
```

Vous êtes invité à entrer un mot de passe.

vSphere Authentication Proxy place en mémoire cache ce nom d'utilisateur et ce mot de passe. Vous pouvez supprimer et recréer l'utilisateur en fonction des besoins. Le domaine doit être accessible au moyen de DNS, mais ne doit pas nécessairement être une source d'identité vCenter Single Sign-On.

vSphere Authentication Proxy reprend le nom d'utilisateur spécifié par *user* pour créer les comptes destinés aux hôtes ESXi dans Active Directory. Par conséquent, l'utilisateur doit disposer de privilèges suffisants pour créer des comptes dans le domaine Active Directory auquel vous ajoutez les hôtes. Lors de la rédaction de ce manuel, l'article 932455 de la base de connaissances Microsoft disposait des informations nécessaires concernant les privilèges de création de compte.

5 Si vous décidez par la suite de supprimer les informations relatives au domaine et à l'utilisateur de vSphere Authentication Proxy, exécutez la commande suivante.

```
camconfig remove-domain -d domain
```

Utiliser vSphere Authentication Proxy pour ajouter un hôte à un domaine

Le serveur Auto Deploy ajoute tous les hôtes qu'il provisionne à vSphere Authentication Proxy, et vSphere Authentication Proxy ajoute ces hôtes au domaine. Si vous voulez ajouter d'autres hôtes à un domaine à l'aide de vSphere Authentication Proxy, vous pouvez ajouter explicitement ces hôtes à vSphere Authentication Proxy. Le serveur vSphere Authentication Proxy ajoute ensuite ces hôtes au domaine. Par conséquent, les informations d'identification fournies par l'utilisateur n'ont plus besoin d'être transmises au système vCenter Server.

Vous pouvez entrer le nom de domaine de l'une des deux façons suivantes :

- **`name.tld`** (par exemple, **`domain.com`**): Le compte est créé sous le récipient par défaut.
- **`name.tld/container/path`** (par exemple, **`domain.com/OU1/OU2`**) : Le compte est créé sous une unité d'organisation (OU) précise.

Prérequis

- Si ESXi utilise un certificat signé par VMCA, vérifiez que l'hôte a été ajouté à vCenter Server. Dans le cas contraire, le service Authentication Proxy ne peut pas approuver l'hôte ESXi.
- Si ESXi utilise un certificat signé par l'autorité de certification, vérifiez que ce certificat a été ajouté à vCenter Server. Reportez-vous à « Gestion de certificats pour les hôtes ESXi », page 52.

Procédure

1 Connectez-vous à un système vCenter Server avec vSphere Web Client.

2 Accédez à l'hôte dans vSphere Web Client et cliquez sur **Configurer**.

3 Sous **Paramètres**, sélectionnez **Services d'authentification**.

4 Cliquez sur **Joindre le domaine**.

5 Entrez un domaine.

Utilisez le formulaire **`name.tld`**, par exemple **`mydomain.com`**, ou **`name.tld/container/path`**, par exemple, **`mydomain.com/organizational_unit1/organizational_unit2`**.

6 Sélectionnez **Utilisation du serveur proxy**.

7 Entrez l'adresse IP du serveur Authentication Proxy, qui est toujours la même que l'adresse IP du système vCenter Server.

8 Cliquez sur **OK**.

Activer l'authentification du client pour vSphere Authentication Proxy

Par défaut, vSphere Authentication Proxy ajoute les hôtes lorsqu'il dispose de leur adresse dans sa liste de contrôle d'accès. Pour une sécurité renforcée, vous pouvez activer l'authentification du client. Lorsque l'authentification du client est activée, vSphere Authentication Proxy vérifie également le certificat de l'hôte.

Prérequis

- Assurez-vous que le système vCenter Server considère l'hôte comme fiable. Par défaut, lorsque vous ajoutez un hôte dans vCenter Server, cet hôte est associé à un certificat qui est signé par une autorité de certification racine fiable de vCenter Server. vSphere Authentication Proxy fait confiance à l'autorité de certification racine fiable de vCenter Server.
- Si vous prévoyez de remplacer les certificats ESXi dans votre environnement, effectuez ce remplacement avant d'activer vSphere Authentication Proxy. Les certificats de l'hôte ESXi doivent correspondre à ceux de l'enregistrement de l'hôte.

Procédure

1 Connectez-vous à vCenter Server Appliance ou à la machine Windows sur laquelle vCenter Server est installé en tant qu'utilisateur avec des privilèges d'administrateur.

2 Exécutez la commande pour activer l'accès à l'interpréteur de commandes de dépistage.

```
shell
```

3 Accédez au répertoire dans lequel le script **camconfig** se trouve.

SE	Emplacement
Dispositif vCenter Server	`/usr/lib/vmware-vmcam/bin/`
vCenter Server sous Windows	`C:\Program Files\VMware\CIS\vmcamd\`

4 L'exécution de la commande suivante permet d'activer l'authentification du client.

```
camconfig ssl-cliAuth -e
```

Ensuite, vSphere Authentication Proxy vérifie le certificat de tout nouvel hôte.

5 Si vous décidez par la suite de désactiver l'authentification de l'hôte, exécutez la commande suivante.

```
camconfig ssl-cliAuth -n
```

Importez le certificat vSphere Authentication Proxy sur l'hôte ESXi

Par défaut, les hôtes ESXi nécessitent une vérification explicite du certificat vSphere Authentication Proxy. Si vous utilisez vSphere Auto Deploy, le service Auto Deploy se charge d'ajouter le certificat dans les hôtes qu'il provisionne. Pour les autres hôtes, vous devez ajouter le certificat de façon explicite.

Prérequis

- Télécharger le certificat de vSphere Authentication Proxy sur l'hôte ESXi Vous pouvez rechercher le certificat à l'emplacement suivant :

vCenter Server Appliance	`/var/lib/vmware/vmcam/ssl/rui.crt`
vCenter Server pour Windows	`C:\ProgramData\VMware\vCenterServer\data\vmcamd\ssl\rui.crt`

- Assurez-vous que le paramètre avancé `UserVars.ActiveDirectoryVerifyCAMCertificate` ESXi est défini sur 1 (valeur par défaut).

Procédure

1. Dans vSphere Web Client, sélectionnez l'hôte ESXi et cliquez sur **Configurer**.
2. Dans la section **Système**, sélectionnez **Services d'authentification**.
3. Cliquez sur **Importer un certificat**.
4. Tapez le chemin du fichier de certificat au format `[`*`banque de données`*`]`*`/chemin/nomcertif`*`.crt` et cliquez sur **OK**.

Générer un nouveau certificat pour vSphere Authentication Proxy

Si vous souhaitez générer un nouveau certificat provisionné par VMCA, ou un nouveau certificat incluant VMCA en tant que certificat subordonné, appliquez les instructions de cette rubrique.

Reportez-vous à « Configurer vSphere Authentication Proxy pour utiliser des certificats personnalisés », page 93 si vous souhaitez utiliser des certificats personnalisés qui sont signés par une autorité de certification tierce ou d'entreprise.

Prérequis

Vous devez disposer de privilèges racine ou d'administration dans le système qui sert à exécuter vSphere Authentication Proxy.

Procédure

1. Créez une copie de `certool.cfg`.

   ```
   cp /usr/lib/vmware-vmca/share/config/certool.cfg /var/lib/vmware/vmcam/ssl/vmcam.cfg
   ```

2. Modifiez cette copie avec des informations sur votre organisation, comme dans l'exemple suivant.

   ```
   Country = IE
   Name = vmcam
   Organization = VMware
   OrgUnit = vTSU
   State = Cork
   Locality = Cork
   Hostname = test-cam-1.test1.vmware.com
   ```

3 Générez la nouvelle clé privée dans `/var/lib/vmware/vmcam/ssl/`.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=/var/lib/vmware/vmcam/ssl/rui.key --
pubkey=/tmp/vmcam.pub --server=localhost
```

Pour *localhost*, fournissez le nom de domaine complet de Platform Services Controller.

4 Générez le nouveau certificat dans `/var/lib/vmware/vmcam/ssl/`, en utilisant la clé et le fichier `vmcam.cfg` que vous avez créés au cours des étapes 1 et 2.

```
/usr/lib/vmware-vmca/bin/certool --server=localhost --gencert --
privkey=/var/lib/vmware/vmcam/ssl/rui.key --cert=/var/lib/vmware/vmcam/ssl/rui.crt --
config=/var/lib/vmware/vmcam/ssl/vmcam.cfg
```

Pour *localhost*, fournissez le nom de domaine complet de Platform Services Controller.

Configurer vSphere Authentication Proxy pour utiliser des certificats personnalisés

Pour utiliser des certificats personnalisés avec vSphere Authentication Proxy, vous générez un CSR, vous l'envoyez à votre autorité de certification pour signature, puis vous placez le certificat signé et le fichier de clé dans en emplacement auquel vSphere Authentication Proxy peut accéder.

Par défaut, vSphere Authentication Proxy génère un CSR lors du premier démarrage et demande à VMCA de signer ce CSR. vSphere Authentication Proxy s'enregistre avec vCenter Server à l'aide de ce certificat. Vous pouvez utiliser des certificats personnalisés dans votre environnement, si vous ajoutez ces certificats à vCenter Server.

Procédure

1 Générez un CSR pour vSphere Authentication Proxy.

a Créez un fichier de configuration, `/var/lib/vmware/vmcam/ssl/vmcam.cfg`, comme dans l'exemple suivant.

```
[ req ]
distinguished_name = req_distinguished_name
encrypt_key = no
prompt = no
string_mask = nombstr
req_extensions = v3_req
[ v3_req ]
basicConstraints = CA:false
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = DNS:olearyf-static-1.csl.vmware.com
[ req_distinguished_name ]
countryName = IE
stateOrProvinceName = Cork
localityName = Cork
0.organizationName = VMware
organizationalUnitName = vTSU
commonName = test-cam-1.test1.vmware.com
```

b Exécutez `openssl` pour générer un fichier CSR et un fichier de clé, en transitant par le fichier de configuration.

```
openssl req -new -nodes -out vmcam.csr -newkey rsa:2048 -
keyout /var/lib/vmware/vmcam/ssl/rui.key -config /var/lib/vmware/vmcam/ssl/vmcam.cfg
```

2 Sauvegardez le certificat `rui.crt`, ainsi que les fichiers `rui.key`, qui sont stockés à l'emplacement suivant.

SE	Emplacement
vCenter Server Appliance	`/var/lib/vmware/vmcam/ssl/rui.crt`
vCenter Server pour Windows	`C:\ProgramData\VMware\vCenterServer\data\vmcamd\ssl\rui.crt`

3 Annulez l'enregistrement de vSphere Authentication Proxy.

a Accédez au répertoire dans lequel le script `camregister` se trouve.

SE	Commandes
vCenter Server Appliance	`/var/lib/vmware-vmcam/bin`
vCenter Server pour Windows	`C:\ProgramData\VMware\vCenterServer\data\vmcamd\ssl\rui.crt`

b Exécutez la commande suivante.

```
camregister --unregister -a VC_address -u user
```

user doit être un utilisateur vCenter Single Sign-On disposant d'autorisations d'administrateur sur vCenter Server.

4 Arrêtez le service vSphere Authentication Proxy.

Outil	Étapes
vSphere Web Client	a Cliquez sur **Administration**, puis sur **Configuration système** sous **Déploiement**. b Cliquez sur **Services**, puis sur le service **VMware vSphere Authentication Proxy** et arrêtez le service.
CLI	`service-control --stop vmcam`

5 Remplacez le certificat `rui.crt` et les fichiers `rui.key` existants par les fichiers que vous avez reçus de votre autorité de certification.

6 Redémarrez le service vSphere Authentication Proxy.

7 Réenregistrez vSphere Authentication Proxy explicitement avec vCenter Server à l'aide du nouveau certificat et de la nouvelle clé en exécutant la commande suivante.

```
camregister --register -a VC_address -u user -c full_path_to_rui.crt -k full_path_to_rui.key
```

Configuration de l'authentification par carte à puce pour ESXi

Vous pouvez utiliser l'authentification par carte à puce pour vous connecter à l'interface DCUI (Direct Console User Interface) ESXi à l'aide d'une carte à puce PIV (Personal Identity Verification), CAC (Common Access Card) ou SC650 au lieu d'entrer un nom d'utilisateur et un mot de passe.

Une carte à puce est une petite carte en plastique dotée d'une puce de circuit intégré. Beaucoup d'organismes publics et de grandes entreprises utilisent l'authentification à deux facteurs basée sur carte à puce pour renforcer la sécurité de leurs systèmes et respecter les réglementations de sécurité.

Lorsque l'authentification par carte à puce est activée sur un hôte ESXi, l'interface DCUI vous invite à entrer une combinaison valide de carte à puce et de code PIN. Cette invite remplace l'invite par défaut qui demande d'entrer un nom d'utilisateur et un mot de passe.

1 Lorsque vous insérez la carte à puce dans le lecteur de carte à puce, l'hôte ESXi lit les informations d'identification qui s'y trouvent.

2 L'interface DCUI ESXi affiche votre ID de connexion et vous invite à entrer votre code PIN.

3 Une fois que vous avez entré le PIN, l'hôte ESXi établit la correspondance entre celui-ci et le PIN stocké sur la carte à puce et vérifie le certificat de la carte à puce à l'aide d'Active Directory.

4 Une fois le certificat de la carte à puce vérifié, ESXi vous connecte à l'interface DCUI.

Si vous préférez passer à l'authentification par nom d'utilisateur et mot de passe via l'interface DCUI, appuyez sur F3.

La puce de la carte se verrouille si vous entrez plusieurs codes PIN incorrects consécutifs (trois, en général). Si une carte à puce est verrouillée, seul le personnel sélectionné peut la déverrouiller.

Activer l'authentification par carte à puce

Activez l'authentification par carte à puce afin de demander aux utilisateurs d'entrer une combinaison de carte à puce et de PIN pour se connecter à l'interface DCUI ESXi.

Prérequis

- Configurez l'infrastructure de manière à prendre en charge l'authentification par carte à puce, avec par exemple des comptes dans le domaine Active Directory, des lecteurs de cartes à puce et des cartes à puce.
- Configurez ESXi pour joindre un domaine Active Directory qui prend en charge l'authentification par carte à puce. Pour plus d'informations, consultez « Utilisation d'Active Directory pour gérer des utilisateurs ESXi », page 86.
- Utilisez vSphere Web Client pour ajouter des certificats racines. Reportez-vous à « Gestion de certificats pour les hôtes ESXi », page 52.

Procédure

1 Dans vSphere Web Client, accédez à l'hôte

2 Cliquez sur **Configurer**.

3 Sous Système, sélectionnez **Services d'authentification**.

Vous voyez l'état actuel de l'authentification par carte à puce et la liste des certificats importés.

4 Dans le panneau Authentification par carte à puce, cliquez sur **Modifier**.

5 Dans la boîte de dialogue Modifier les paramètres d'authentification par carte à puce, sélectionnez la page Certificats.

6 Ajoutez des certificats d'autorité de certification (CA) approuvés (certificats CA racines et intermédiaires, par exemple).

7 Ouvrez la page Authentification par carte à puce, cochez la case **Activer l'authentification par carte à puce** et cliquez sur **OK**.

Désactiver l'authentification par carte à puce

Désactiver l'authentification par carte à puce pour revenir à l'authentification par nom d'utilisateur et mot de passe par défaut pour la connexion à l'interface DCUI d'ESXi.

Procédure

1 Dans vSphere Web Client, accédez à l'hôte

2 Cliquez sur **Configurer**.

3 Sous Système, sélectionnez **Services d'authentification**.

Vous voyez l'état actuel de l'authentification par carte à puce et la liste des certificats importés.

4 Dans le panneau Authentification par carte à puce, cliquez sur **Modifier**.

5 Sur la page Authentification par carte à puce, décochez la case **Activer l'authentification par carte à puce**, puis cliquez sur **OK**.

S'authentifier avec le nom d'utilisateur et le mot de passe en cas de problèmes de connectivité

Si le serveur de domaine Active Directory (AD) n'est pas accessible, vous pouvez vous connecter à l'interface DCUI ESXi avec l'authentification par nom d'utilisateur et mot de passe pour réaliser des opérations de secours sur l'hôte.

Exceptionnellement, il est possible que le serveur de domaine AD ne soit pas accessible pour authentifier les informations d'identification de l'utilisateur sur la carte à puce, par exemple suite à des problèmes de connectivité, à une panne de réseau ou à un sinistre. Dans ce cas, vous pouvez vous connecter à l'interface DCUI ESXi en utilisant les informations d'identification d'un utilisateur administrateur local d'ESXi. Une fois connecté, vous pouvez exécuter des diagnostics ou toute autre mesure d'urgence. Le recours à la connexion par nom d'utilisateur et mot de passe est consigné. Une fois la connectivité avec Active Directory restaurée, l'authentification par carte à puce est réactivée.

Remarque La perte de connectivité réseau avec vCenter Server n'affecte pas l'authentification par carte à puce si le serveur de domaine Active Directory (AD) est disponible.

Utilisation de l'authentification par carte à puce en mode de verrouillage

Lorsqu'il est activé, le mode de verrouillage sur l'hôte ESXi renforce la sécurité de l'hôte et limite l'accès à l'interface DCUI. Le mode de verrouillage peut désactiver la fonctionnalité d'authentification par carte à puce.

En mode de verrouillage normal, seuls les utilisateurs répertoriés dans la liste des utilisateurs exceptionnels et disposant de privilèges d'administration peuvent accéder à l'interface DCUI. Les utilisateurs exceptionnels sont des utilisateurs locaux d'un hôte ou des utilisateurs Active Directory disposant d'autorisations définies localement pour l'hôte ESXi. Si vous souhaitez utiliser l'authentification par carte à puce en mode de verrouillage normal, vous devez ajouter les utilisateurs à la liste des utilisateurs exceptionnels à partir de vSphere Web Client. Lorsque l'hôte passe en mode de verrouillage normal, ces utilisateurs ne perdent pas leurs autorisations et peuvent se connecter à l'interface DCUI. Pour plus d'informations, consultez « Spécifier les utilisateurs exceptionnels du mode de verrouillage », page 82.

En mode de verrouillage strict, le service DCUI est interrompu. Il est donc impossible d'utiliser l'authentification par carte à puce pour accéder à l'hôte.

Utilisation de ESXi Shell

Le ESXi Shell est désactivé par défaut sur les hôtes ESXi. Vous pouvez activer l'accès local et distant au shell si nécessaire.

Activez le ESXi Shell uniquement à des fins de dépannage. Le ESXi Shell est indépendant du mode verrouillage. Le fait que l'hôte fonctionne en mode verrouillage ne vous empêche pas d'activer ou de désactiver ESXi Shell.

ESXi Shell	Activez ce service pour accéder localement au ESXi Shell.
SSH	Activez ce service pour accéder à ESXi Shell à distance en utilisant SSH.

Voir *Sécurité vSphere*.

Interface utilisateur de la console directe (DCUI)	Lorsque vous activez ce service en mode verrouillage, vous pouvez vous connecter localement à l'interface utilisateur de la console directe en tant qu'utilisateur racine, puis désactiver le mode verrouillage. Vous pouvez ensuite accéder à l'hôte via une connexion directe à VMware Host Client ou en activant ESXi Shell.

L'utilisateur racine et les utilisateurs disposant du rôle d'administrateur peuvent accéder au ESXi Shell. Les utilisateurs du groupe Active Directory ESX Admins reçoivent automatiquement le rôle d'Administrateur. Par défaut, seul l'utilisateur racine peut exécuter des commandes système (telles que `vmware -v`) en utilisant ESXi Shell.

Remarque N'activez pas le ESXi Shell si n'avez pas réellement besoin d'un accès.

- Utiliser vSphere Web Client pour activer l'accès à ESXi Shell page 97

  Vous pouvez utiliser vSphere Web Client pour activer un accès local et distant (SSH) au service ESXi Shell et pour définir le délai d'attente d'inactivité et le délai d'attente de disponibilité.

- Utiliser l'interface utilisateur de la console directe (DCUI) pour activer l'accès au service ESXi Shell page 99

  L'interface utilisateur de la console directe (DCUI) vous permet d'interagir avec l'hôte localement en utilisant des menus textuels. Évaluez avec soin si les exigences de votre environnement en matière de sécurité permettent l'activation de l'interface utilisateur de la console directe (DCUI).

- Connexion au ESXi Shell pour une opération de dépannage page 100

  Effectuez des tâches de configuration d'ESXi avec vSphere Web Client, vSphere CLI ou vSphere PowerCLI. Connectez-vous au ESXi Shell (anciennement mode support technique ou TSM) uniquement à des fins de dépannage.

Utiliser vSphere Web Client pour activer l'accès à ESXi Shell

Vous pouvez utiliser vSphere Web Client pour activer un accès local et distant (SSH) au service ESXi Shell et pour définir le délai d'attente d'inactivité et le délai d'attente de disponibilité.

Remarque Accédez à l'hôte à l'aide de vSphere Web Client, d'outils de ligne de commande à distance (vCLI et PowerCLI) et d'API publiées. N'activez pas l'accès à distance à l'hôte à l'aide de SSH, sauf si des circonstances spéciales imposent l'activation de l'accès SSH.

Prérequis

Si vous souhaitez utiliser une clé SSH autorisée, vous pouvez la télécharger. Reportez-vous à la section « Clés SSH ESXi », page 47.

Procédure

1. Accédez à l'hôte dans l'inventaire de vSphere Web Client.
2. Cliquez sur **Configurer**.
3. Dans Système, sélectionnez **Profil de sécurité**.
4. Dans le panneau Services, cliquez sur **Modifier**.
5. Sélectionnez un service dans la liste.
   - ESXi Shell
   - SSH
   - Interface utilisateur de la console directe

6 Cliquez sur **Détails du service** et sélectionnez la règle de démarrage **Démarrer et arrêter manuellement**.

   Lorsque vous sélectionnez **Démarrer et arrêter manuellement**, le service ne démarre pas lorsque vous redémarrez l'hôte. Si vous voulez démarrer le service lors du redémarrage de l'hôte, sélectionnez **Démarrer et arrêter avec hôte**.

7 Sélectionnez **Démarrer** pour activer le service.

8 Cliquez sur **OK**.

Suivant

Définissez le délai d'attente de disponibilité et le délai d'inactivité pour ESXi Shell. Reportez-vous à « Créer un délai d'attente de disponibilité pour ESXi Shell dans vSphere Web Client », page 98 et « Créer un délai d'expiration pour les sessions ESXi Shell inactives dans vSphere Web Client », page 98

Créer un délai d'attente de disponibilité pour ESXi Shell dans vSphere Web Client

ESXi Shell est désactivé par défaut. Vous pouvez paramétrer un délai d'attente de disponibilité pour ESXi Shell pour renforcer la sécurité quand vous activez le shell.

La valeur du délai d'attente de disponibilité correspond au temps qui peut s'écouler avant de vous connecter suite à l'activation de ESXi Shell. Lorsque le délai est écoulé, le service est désactivé et les utilisateurs ne peuvent plus se connecter.

Procédure

1 Accédez à l'hôte dans l'inventaire de vSphere Web Client.

2 Cliquez sur **Configurer**..

3 Dans Système, sélectionnez **Paramètres système avancés**.

4 Sélectionnez UserVars.ESXiShellTimeOut, puis cliquez sur **Modifier**.

5 Saisissez le paramètre de délai d'inactivité.

   Vous devez redémarrer le service SSH et le service ESXi Shell pour que le délai soit pris en compte.

6 Cliquez sur **OK**.

Si vous avez ouvert une session au moment de l'expiration de ce délai, elle restera ouverte. Cependant, une fois que vous vous êtes déconnecté ou que votre session est terminée, les utilisateurs ne sont plus autorisés à se connecter.

Créer un délai d'expiration pour les sessions ESXi Shell inactives dans vSphere Web Client

Si un utilisateur active ESXi Shell sur un hôte mais oublie de se déconnecter de la session, la session inactive demeure connectée indéfiniment. La connexion ouverte peut augmenter les possibilités qu'une personne obtienne un accès privilégié à l'hôte. Vous pouvez éviter cela en paramétrant un délai d'expiration des sessions inactives.

Le délai d'expiration d'inactivité correspond à la période au terme de laquelle un utilisateur est déconnecté d'une session interactive inactive. Vous pouvez définir ce délai pour les sessions locales et distantes (SSH) dans l'interface de la console directe (DCUI) ou dans vSphere Web Client.

Procédure

1 Accédez à l'hôte dans l'inventaire de vSphere Web Client.

2 Cliquez sur **Configurer**..

3 Dans Système, sélectionnez **Paramètres système avancés**.

4 Sélectionnez UserVars.ESXiShellInteractiveTimeOut, cliquez sur l'icône **Modifier** et saisissez le paramètre du délai d'expiration.

5 Redémarrez le service ESXi Shell et le service SSH pour que le délai d'expiration prenne effet.

Si la session est inactive, les utilisateurs sont déconnectés à l'expiration du délai d'attente.

Utiliser l'interface utilisateur de la console directe (DCUI) pour activer l'accès au service ESXi Shell

L'interface utilisateur de la console directe (DCUI) vous permet d'interagir avec l'hôte localement en utilisant des menus textuels. Évaluez avec soin si les exigences de votre environnement en matière de sécurité permettent l'activation de l'interface utilisateur de la console directe (DCUI).

Vous pouvez utiliser l'interface utilisateur de la console directe pour activer l'accès local et distant au service ESXi Shell.

Remarque Les modifications apportées à l'hôte en utilisant l'interface utilisateur de la console directe, vSphere Web Client, ESXCLI ou d'autres outils d'administration sont enregistrées dans un stockage permanent toutes les heures ou lors d'un arrêt dans les règles. Les modifications peuvent se perdre si l'hôte échoue avant qu'elles ne soient enregistrées.

Procédure

1 Dans l'interface utilisateur de la console directe, appuyez sur F2 pour accéder au menu Personnalisation du système.

2 Sélectionnez **Options de dépannage** et appuyez sur Entrée.

3 Dans le menu des options de mode de dépannage, sélectionnez un service à activer.

- Activer ESXi Shell
- Activer SSH

4 Appuyez sur Entrée pour activer le service souhaité.

5 Appuyez sur Échap jusqu'à ce que vous reveniez au menu principal de l'interface utilisateur de la console directe.

Suivant

Définissez le délai d'attente de disponibilité et le délai d'inactivité du service ESXi Shell. Voir « Créer un délai d'attente de disponibilité pour ESXi Shell dans l'interface utilisateur de console directe », page 99 et « Créer un délai d'expiration pour des sessions ESXi Shell inactives », page 100.

Créer un délai d'attente de disponibilité pour ESXi Shell dans l'interface utilisateur de console directe

ESXi Shell est désactivé par défaut. Vous pouvez paramétrer un délai d'attente de disponibilité pour ESXi Shell pour renforcer la sécurité quand vous activez le shell.

La valeur du délai d'attente de disponibilité correspond au temps qui peut s'écouler avant de vous connecter suite à l'activation de ESXi Shell. Lorsque le délai est écoulé, le service est désactivé et les utilisateurs ne peuvent plus se connecter.

Procédure

1 Dans le menu des options de mode de dépannage, sélectionnez **Modifier les délais d'ESXi Shell et de SSH** et cliquez sur Entrée.

2 Entrez le délai d'attente de disponibilité.

   Vous devez redémarrer le service SSH et le service ESXi Shell pour que le délai soit pris en compte.

3 Appuyez sur Entrée et Échap jusqu'à ce que vous reveniez au menu principal de l'interface utilisateur de console directe.

4 Cliquez sur **OK**.

Si vous avez ouvert une session au moment de l'expiration de ce délai, elle restera ouverte. Cependant, une fois que vous vous êtes déconnecté ou que votre session est terminée, les utilisateurs ne sont plus autorisés à se connecter.

Créer un délai d'expiration pour des sessions ESXi Shell inactives

Si un utilisateur active ESXi Shell sur un hôte mais oublie de se déconnecter de la session, la session inactive demeure connectée indéfiniment. La connexion ouverte peut augmenter les possibilités qu'une personne obtienne un accès privilégié à l'hôte. Vous pouvez éviter cela en paramétrant un délai d'expiration des sessions inactives.

Le délai d'inactivité correspond au temps qui peut s'écouler avant que l'utilisateur ne soit déconnecté d'une session interactive inactive. Les modifications du délai d'inactivité s'appliquent lors de la prochaine connexion de l'utilisateur à ESXi Shell. Les modifications n'ont pas d'incidence sur les sessions existantes.

Vous pouvez spécifier le délai d'expiration en secondes dans l'interface DCUI (Direct Console User Interface) ou en minutes dans vSphere Web Client.

Procédure

1 Dans le menu des options de mode de dépannage, sélectionnez **Modifier les délais d'ESXi Shell et de SSH** et cliquez sur Entrée.

2 Entrez le délai d'expiration en secondes.

   Vous devez redémarrer le service SSH et le service ESXi Shell pour que le délai soit pris en compte.

3 Appuyez sur Entrée et Échap jusqu'à ce que vous reveniez au menu principal de l'interface utilisateur de console directe.

Si la session est inactive, les utilisateurs sont déconnectés à l'expiration du délai d'attente.

Connexion au ESXi Shell pour une opération de dépannage

Effectuez des tâches de configuration d'ESXi avec vSphere Web Client, vSphere CLI ou vSphere PowerCLI. Connectez-vous au ESXi Shell (anciennement mode support technique ou TSM) uniquement à des fins de dépannage.

Procédure

1 Connectez-vous au ESXi Shell en utilisant l'une des méthodes suivantes.

   - Si vous avez un accès direct à l'hôte, appuyez sur la combinaison de touches Alt+F1 pour ouvrir la page de connexion de la console physique de la machine.
   - Si vous vous connectez à l'hôte à distance, utilisez SSH ou une autre connexion à distance pour ouvrir une session sur l'hôte.

2 Entrez un nom d'utilisateur et un mot de passe reconnus par l'hôte.

Démarrage sécurisé UEFI des hôtes ESXi

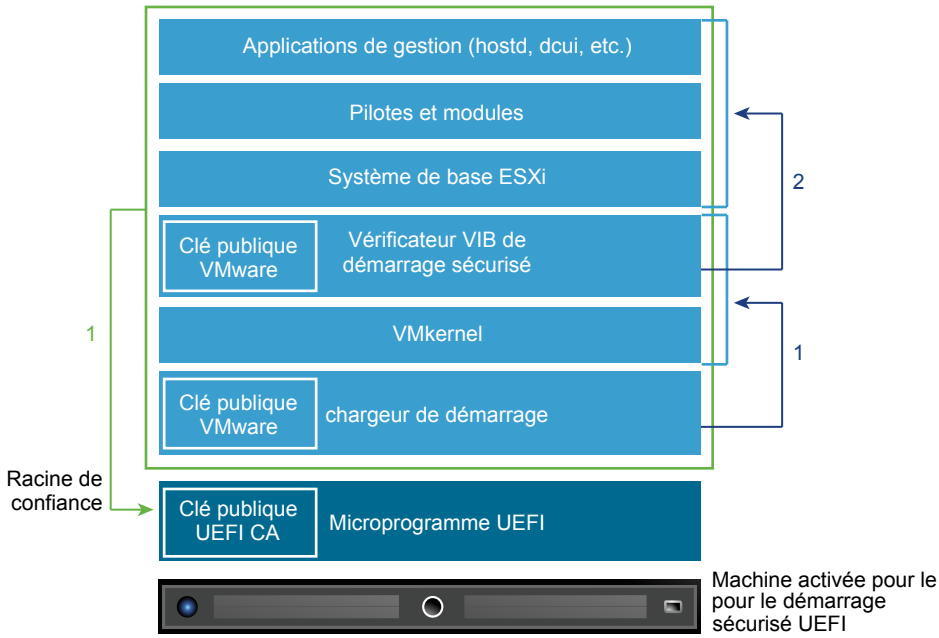
Le démarrage sécurisé est une fonctionnalité standard du microprogramme UEFI. Lorsque le démarrage sécurisé est activé, si le chargeur de démarrage du système d'exploitation n'est pas signé par chiffrement, la machine refuse de charger un pilote ou une application UEFI. À partir de vSphere 6.5, ESXi prend en charge le démarrage sécurisé s'il est activé dans le matériel.

Présentation du démarrage sécurisé UEFI

ESXi 6.5 et versions ultérieures prend en charge le démarrage sécurisé UEFI à chaque niveau de la pile de démarrage pour .

Remarque Avant d'utiliser le démarrage sécurisé UEFI sur un hôte qui a été mis à niveau vers ESXi 6.5, vérifiez la compatibilité en suivant les instructions dans « Exécuter le script de validation du démarrage sécurisé sur un hôte ESXi mis à niveau », page 102. Si vous mettez à niveau un hôte ESXi en utilisant les commandes `esxcli`, la mise à niveau ne prend pas en charge le chargeur de démarrage. Dans ce cas, vous ne pouvez pas effectuer de démarrage sécurisé sur le système.

Figure 3-1. Démarrage sécurisé UEFI



Lorsque le démarrage sécurisé est activé, la séquence de démarrage se déroule de la manière suivante.

1. À partir de vSphere 6.5, le chargeur de démarrage ESXi contient une clé publique VMware. Le chargeur de démarrage utilise cette clé pour vérifier la signature du noyau et un petit sous-ensemble du système incluant un vérificateur VIB de démarrage sécurisé.
2. Le vérificateur VIB vérifie chaque module VIB installé sur le système.

L'ensemble du système est alors démarré, avec la racine d'approbation dans les certificats faisant partie du microprogramme UEFI.

Dépannage du démarrage sécurisé UEFI

Si le démarrage sécurisé échoue à un niveau de la séquence de démarrage, une erreur se produit.

Le message d'erreur dépend du fournisseur du matériel et du niveau où la vérification a échoué.

- Si vous tentez de démarrer la machine avec un chargeur de démarrage non signé ou qui a été falsifié, une erreur se produit lors de la séquence de démarrage. Le message exact dépend du fournisseur du matériel. Il peut être similaire au message d'erreur suivant.

  ```
  UEFI0073: Unable to boot PXE Device...because of the Secure Boot policy
  ```

- Si le noyau a été falsifié, une erreur similaire à la suivante se produit.

  ```
  Fatal error: 39 (Secure Boot Failed)
  ```

- Si un module (VIB ou pilote) a été falsifié, un écran violet avec le message suivant s'affiche.

  ```
  UEFI Secure Boot failed:
  Failed to verify signatures of the following vibs (XX)
  ```

Pour résoudre les problèmes de démarrage sécurisé, suivez la procédure suivante.

1 Redémarrez l'hôte avec le démarrage sécurisé désactivé.

2 Exécutez le script de vérification du démarrage sécurisé (voir « Exécuter le script de validation du démarrage sécurisé sur un hôte ESXi mis à niveau », page 102).

3 Examinez les informations dans le fichier `/var/log/esxupdate.log`.

Exécuter le script de validation du démarrage sécurisé sur un hôte ESXi mis à niveau

Si votre matériel prend en charge le démarrage sécurisé UEFI, vous devriez être en mesure d'activer le démarrage sécurisé de l'hôte ESXi. Cela est possible ou non, selon la manière dont vous avez effectué la mise à niveau. Pour savoir si le démarrage sécurisé est pris en charge, vous pouvez exécuter un script de validation après avoir effectué la mise à niveau.

Le démarrage sécurisé UEFI nécessite que les signatures VIB d'origine soient persistantes. Les anciennes versions de ESXi ne conservent pas les signatures, mais le processus de mise à niveau met à jour les signatures VIB.

- Si vous effectuez la mise à niveau en utilisant ISO, les VIB mis à niveau ont des signatures persistantes.
- Si vous effectuez la mise à niveau en utilisant les commandes ESXCLI, les VIB mis à niveau ne comportent pas de signatures persistantes. Dans ce cas, vous ne pouvez pas effectuer de démarrage sécurisé sur le système.

Même si vous effectuez la mise à niveau en utilisant ISO, le processus de mise à niveau ne peut pas conserver les signatures des VIB tiers. Dans ce cas, le démarrage sécurisé sur le système échoue.

Remarque

Le démarrage sécurisé UEFI nécessite également un chargeur de démarrage à jour. Ce script ne vérifie pas si le chargeur de démarrage est à jour.

Prérequis

- Vérifiez si le matériel prend en charge le démarrage sécurisé UEFI.
- Vérifiez si tous les VIB sont signés avec le niveau d'acceptation minimum PartnerSupported. Si vous incluez des VIB au niveau CommunitySupported, vous ne pouvez pas utiliser le démarrage sécurisé.

Procédure

1 Mettez à niveau le dispositif ESXi et exécutez la commande suivante.

```
/usr/lib/vmware/secureboot/bin/secureBoot.py –c
```

2 Vérifiez le résultat.

Le résultat inclut `Secure boot can be enabled` ou `Secure boot CANNOT be enabled`.

Fichiers journaux ESXi

Les fichiers journaux constituent un élément important dans le dépannage des attaques et l'obtention d'informations relatives aux failles. Une journalisation effectuée sur un serveur dédié centralisé et sécurisé peut contribuer à éviter la falsification des journaux. La journalisation à distance fournit également un enregistrement des contrôles à long terme.

Prenez les mesures suivantes pour renforcer la sécurité de l'hôte.

- Configurez la journalisation permanente d'une banque de données. Les journaux des hôtes ESXi sont stockés par défaut dans le système de fichiers en mémoire. Par conséquent, ils sont perdus lorsque vous redémarrez l'hôte et seules 24 heures de données de journalisation sont stockées. Lorsque vous activez la journalisation permanente, vous obtenez un enregistrement dédié de l'activité de l'hôte.
- La connexion à distance à un hôte central vous permet de rassembler les fichiers journaux sur celui-ci. À partir de cet hôte, vous pouvez surveiller tous les hôtes à l'aide d'un outil unique, effectuer une analyse regroupée et rechercher des données dans les journaux. Cette approche facilite la surveillance et révèle des informations sur les attaques coordonnées sur plusieurs hôtes.
- Configurez le protocole syslog sécurisé à distance sur les hôtes ESXi en utilisant une interface de ligne de commande comme vCLI ou PowerCLI ou une API de client.
- Effectuez une requête dans la configuration syslog pour vous assurer que le serveur et le port syslog sont valides.

Pour des informations sur la configuration du protocole syslog, reportez à la documentation *Surveillance et performances de vSphere* sur les fichiers journaux ESXi.

Configurer Syslog sur des hôtes ESXi

Tous les hôtes ESXi exécutent un service syslog (`vmsyslogd`) qui écrit les messages venant de VMkernel et d'autres composants système dans des fichiers journaux.

Vous pouvez utiliser vSphere Web Client ou la commande vCLI `esxcli system syslog` pour configurer le service syslog.

Pour plus d'informations sur l'utilisation de commandes vCLI, reportez-vous à *Démarrage avec vSphere Command-Line Interfaces*.

Procédure

1 Dans l'inventaire de vSphere Web Client, sélectionnez l'hôte.

2 Cliquez sur **Configurer**.

3 Dans Système, cliquez sur **Paramètres système avancés**.

4 Filtre pour **`syslog`**.

5 Pour configurer la journalisation de façon globale, sélectionnez le paramètre à modifier et cliquez sur l'icône **Modifier**.

Option	Description
Syslog.global.defaultRotate	Nombre maximal d'archives à conserver. Vous pouvez définir ce nombre de façon globale et pour les sous-unités d'enregistrement automatique.
Syslog.global.defaultSize	Taille par défaut du journal, en Ko, avant que le système n'effectue la rotation des journaux. Vous pouvez définir ce nombre de façon globale et pour les sous-unités d'enregistrement automatique.

Option	Description
Syslog.global.LogDir	Répertoire dans lequel sont stockés les journaux. Le répertoire peut se trouver sur des volumes NFS ou VMFS montés. Seul le répertoire `/scratch` situé sur le système de fichiers local subsiste après des redémarrages. Spécifiez le répertoire sous la forme [*nom_banque_de_données*]*chemin_du_fichier*, le chemin étant relatif à la racine du volume qui assure la sauvegarde de la banque de données. Par exemple, le chemin `[storage1] /systemlogs` crée un mappage vers le chemin `/ vmfs/volumes/storage1/systemlogs.`
Syslog.global.logDirUnique	Lorsque vous sélectionnez cette option, un sous-répertoire est créé portant le nom de l'hôte ESXi dans le répertoire spécifié par **Syslog.global.LogDir**. Il est utile d'avoir un répertoire unique si le même répertoire NFS est utilisé par plusieurs hôtes ESXi.
Syslog.global.LogHost	Hôte distant vers lequel les messages syslog sont transférés et port sur lequel l'hôte distant reçoit les messages syslog. Vous pouvez inclure le protocole et le port, par exemple, `ssl://hostName1:1514`. Les protocoles UDP (par défaut), TCP et SSL sont pris en charge. L'hôte distant doit avoir un syslog installé et correctement configuré pour recevoir les messages syslog transférés. Consultez la documentation du service syslog installé sur l'hôte distant pour plus d'informations sur la configuration.

6 (Facultatif) Pour remplacer la taille par défaut et la rotation des journaux d'un journal quelconque.

   a Cliquez sur le nom du journal que vous souhaitez personnaliser.

   b Cliquez sur l'icône **Modifier** et entrez le nombre de rotations et la taille de journal souhaités.

7 Cliquez sur **OK**.

Les modifications apportées aux options syslog prennent effet immédiatement.

Emplacements des fichiers journaux ESXi

ESXi enregistre l'activité de l'hôte dans des fichiers journaux en utilisant un outil syslog.

Composant	Emplacement	Objectif
VMkernel	`/var/log/vmkernel.log`	Enregistre les activités relatives aux machines virtuelles et à ESXi.
Avertissements VMkernel	`/var/log/vmkwarning.log`	Enregistre les activités relatives aux machines virtuelles.
Résumé VMkernel	`/var/log/vmksummary.log`	Utilisé pour déterminer les statistiques de temps de fonctionnement et de disponibilité pourESXi (virgule séparée).
Journal de l'agent hôte ESXi	`/var/log/hostd.log`	Contient des informations sur l'agent gérant et configurant les hôtes ESXi et leurs machines virtuelles.
Journal de l'agent vCenter	`/var/log/vpxa.log`	Contient des informations sur l'agent communiquant avec vCenter Server (si l'hôte est géré par vCenter Server).
Journal du shell	`/var/log/shell.log`	Contient un enregistrement de toutes les commandes tapées dans ESXi Shell, ainsi que les événements de shell (par exemple, le moment où le shell a été activé).
Authentification	`/var/log/auth.log`	Contient tous les événements relatifs à l'authentification pour le système local.

Composant	Emplacement	Objectif
Messages système	`/var/log/syslog.log`	Contient tous les messages généraux du journal et peut être utilisé en cas de dépannage. Ces informations étaient précédemment situées dans le fichier journal des messages.
Machines virtuelles	Le même répertoire que les fichiers de configuration de la machine virtuelle, appelés vmware.log et vmware*.log. Par exemple, `/vmfs/volumes/`*`datastore/virtual machine`*`/vwmare.log`	Contient les événements d'alimentation de la machine virtuelle, les informations relatives aux défaillances système, la synchronisation horaire, les modifications virtuelles du matériel, les migrations vMotion, les clones de machines, etc.

Trafic de la journalisation de la tolérance aux pannes

VMware Fault Tolerance (FT) capture les entrées et les événements qui se produisent sur une machine virtuelle principale et les transmet à la machine virtuelle secondaire qui s'exécute sur un autre hôte.

Le trafic de la journalisation entre les machines virtuelles primaires et secondaires est chiffré et contient un réseau client et des données E/S de stockage, ainsi que le contenu de la mémoire du système d'exploitation invité. Ce trafic peut inclure des données sensibles telles que des mots de passe en texte brut. Pour éviter que ces données ne soient divulguées, assurez-vous que ce réseau est sécurisé, notamment pour éviter les attaques « intermédiaires ». Par exemple, vous pouvez utiliser un réseau privé pour le trafic de la journalisation de la tolérance aux pannes.

Sécurisation des systèmes vCenter Server 4

La sécurisation de vCenter Server comporte notamment le fait de veiller à la sécurité de l'hôte sur lequel vCenter Server fonctionne, en respectant les meilleures pratiques en matière d'attribution des privilèges et des rôles, et en vérifiant l'intégrité des clients qui se connectent au vCenter Server.

Ce chapitre aborde les rubriques suivantes :

Meilleures pratiques de sécurité de vCenter Server

Le respect des meilleures pratiques de sécurité de vCenter Server vous aide à garantir l'intégrité de votre environnement vSphere.

Meilleures pratiques pour le contrôle d'accès à vCenter Server

Contrôlez strictement l'accès aux différents composants de vCenter Server pour augmenter la sécurité du système.

Les directives suivantes contribuent à garantir la sécurité de votre environnement.

Utiliser des comptes nommés

- Si le compte d'administrateur Windows local a actuellement le rôle Administrateur pour vCenter Server, supprimez ce rôle et attribuez-le à un ou plusieurs comptes Administrateur de vCenter Server nommés. N'accordez le rôle Administrateur qu'aux administrateurs nommés qui doivent en bénéficier. Vous pouvez créer des rôles personnalisés ou utiliser le rôle Aucun administrateur de chiffrement pour les administrateurs qui disposent de privilèges plus restreints. N'appliquez pas ce privilège à un groupe dont la composition ne fait pas l'objet d'un contrôle strict.

  Remarque À partir de vSphere 6.0, l'administrateur local n'a plus de droits administratifs complets sur vCenter Server par défaut.

- Installez vCenter Server en utilisant un compte de service plutôt qu'un compte Windows. Le compte de service doit être un administrateur sur la machine locale.
- Assurez-vous que les applications utilisent des comptes de service uniques lors d'une connexion à un système vCenter Server.

Surveillez les privilèges des utilisateurs administrateurs de vCenter Server

Certains utilisateurs administrateurs ne doivent pas avoir le rôle Administrateur. Créez plutôt un rôle personnalisé disposant de l'ensemble approprié de privilèges et attribuez-le aux autres administrateurs.

Les utilisateurs disposant du rôle Administrateur de vCenter Server disposent de privilèges sur tous les objets de la hiérarchie. Par exemple, le rôle Administrateur permet par défaut aux utilisateurs d'interagir avec les fichiers et les programmes du système d'exploitation invité de la machine virtuelle. L'attribution de ce rôle à un trop grand nombre d'utilisateurs peut compromettre la confidentialité, la disponibilité ou l'intégrité des données. Créez un rôle qui donne aux administrateurs les privilèges dont ils ont besoin, mais supprimez certains privilèges de gestion de machines virtuelles.

Minimiser l'accès

N'autorisez pas les utilisateurs à se connecter directement à la machine hôte vCenter Server. Les utilisateurs qui sont connectés à la machine hôte vCenter Server peuvent provoquer des dommages, intentionnels ou non, en modifiant les paramètres et les processus. Ils ont également potentiellement accès aux informations d'identification de vCenter (par exemple, le certificat SSL). Autorisez uniquement les utilisateurs ayant des tâches légitimes à effectuer à se connecter au système et assurez-vous que les événements de connexion sont vérifiés.

Accordez des privilèges minimaux aux utilisateurs de base de données vCenter Server

L'utilisateur de la base de données n'a besoin que de quelques privilèges spécifiques à l'accès à la base de données.

Certains privilèges ne sont nécessaires que pour l'installation et la mise à niveau. Après l'installation ou la mise à niveau de vCenter Server, vous pouvez supprimer ces privilèges du rôle d'administrateur de base de données.

Restreindre l'accès au navigateur de la banque de données

Attribuez le privilège **Banque de données.Parcourir la banque de données** uniquement aux utilisateurs ou aux groupes qui en ont réellement besoin. Les utilisateurs qui disposent de ce privilège peuvent afficher, charger ou télécharger les fichiers des banques de données associées au déploiement de vSphere par l'intermédiaire du navigateur Web ou de vSphere Web Client.

Empêcher des utilisateurs d'exécuter des commandes dans une machine virtuelle

Par défaut, un utilisateur avec le rôle Administrateur de vCenter Server peut interagir avec les fichiers et les programmes au sein du système d'exploitation invité d'une machine virtuelle. Afin de réduire les risques d'atteinte à la confidentialité, la disponibilité et l'intégrité de l'invité, créez un rôle d'accès non-invité personnalisé, dépourvu du privilège **Systèmes invités**. Reportez-vous à « Empêcher des utilisateurs d'exécuter des commandes dans une machine virtuelle », page 130.

Envisager de modifier la stratégie de mot de passe pour vpxuser

Par défaut, vCenter Server modifie automatiquement le mot de passe vpxuser tous les 30 jours. Assurez-vous que ce paramètre correspond à la stratégie de l'entreprise ou configurez la stratégie de mot de passe de vCenter Server. Reportez-vous à « Configurer la stratégie de mot de passe de vCenter Server », page 109.

Remarque Assurez-vous que la stratégie d'expiration du mot de passe n'est pas trop courte.

Vérifier les privilèges après le redémarrage de vCenter Server

Vérifiez la réaffectation des privilèges lorsque vous redémarrez vCenter Server. Si l'utilisateur ou le groupe qui a le rôle Administrateur sur le dossier racine ne peut pas être validé lors d'un redémarrage, le rôle est supprimé de cet utilisateur ou de ce groupe. À la place, vCenter Server accordez le rôle Administrateur à l'administrateur de vCenter Single Sign-On (par défaut, administrator@vsphere.local). Ce compte peut alors agir en tant qu'administrateur de vCenter Server.

Rétablissez un compte d'administrateur nommé et attribuez-lui le rôle Administrateur pour éviter d'utiliser le compte d'administrateur de vCenter Single Sign-On anonyme (par défaut, administrator@vsphere.local).

Utiliser des niveaux de chiffrement RDP élevés

Sur chaque ordinateur Windows de l'infrastructure, vérifiez que les paramètres de configuration d'hôte des services Bureau à distance sont définis afin de garantir le niveau de chiffrement le plus élevé pour votre environnement.

Vérifiez les certificats vSphere Web Client

Demander aux utilisateurs d'une application vSphere Web Client ou d'autres applications client de ne jamais ignorer les avertissements de vérification de certificat. Sans vérification de certificat, l'utilisateur peut être sujet à une attaque MiTM.

Configurer la stratégie de mot de passe de vCenter Server

Par défaut, vCenter Server modifie automatiquement le mot de passe vpxuser tous les 30 jours. Vous pouvez modifier cette valeur dans vSphere Web Client.

Procédure

1 Sélectionnez vCenter Server dans la hiérarchie des objets vSphere Web Client.

2 Cliquez sur **Configurer**.

3 Cliquez sur **Paramètres avancés** et entrez **`VimPasswordExpirationInDays`** dans la case des filtres.

4 Configurez `VirtualCenter.VimPasswordExpirationInDays` pour qu'il soit conforme à vos exigences.

Suppression de certificats expirés ou révoqués et de journaux d'installations ayant échoué

La conservation de certificats expirés ou révoqués ou des journaux d'installation de vCenter Server générés lors de l'échec d'une installation sur votre système vCenter Server peut compromettre la sécurité de votre environnement.

La suppression des certificats expirés ou révoqués est nécessaire pour les raisons suivantes.

- Si les certificats expirés ou révoqués ne sont pas supprimés du système vCenter Server, l'environnement peut être exposé à une attaque MiTM.
- Dans certains cas, un fichier journal contenant le mot de passe d'une base de données en texte clair est créé sur le système lors d'un échec d'installation de vCenter Server. Un attaquant qui s'introduit dans le système vCenter Server peut réussir à accéder à ce mot de passe et, en même temps, à la base de données vCenter Server.

Protection de l'hôte Windows vCenter Server

Protégez l'hôte Windows contre les vulnérabilités et les attaques lors de l'exécution de vCenter Server en s'assurant que l'environnement de l'hôte est aussi sécurisé que possible.

- Gérez un système d'exploitation, une base de données ou un matériel pris en charge pour le système vCenter Server. Si vCenter Server ne s'exécute pas sur un système d'exploitation pris en charge, il est possible qu'il ne fonctionne pas correctement, ce qui le rend vulnérable aux attaquesvCenter Server.
- Veillez à ce que les correctifs soient correctement installés sur le système vCenter Server. Le serveur est moins vulnérable aux attaques si les correctifs du système d'exploitation sont mis à jour régulièrement.
- Protégez le système d'exploitation sur l'hôte vCenter Server. La protection comprend un logiciel antivirus et un logiciel anti-programme malveillant.
- Sur chaque ordinateur Windows de l'infrastructure, vérifiez que les paramètres de configuration d'hôte des services Bureau à distance (RDP) sont définis afin de garantir le niveau de chiffrement le plus élevé conformément aux directives standard du marché ou aux instructions internes.

Pour obtenir des informations sur la compatibilité des systèmes d'exploitation et des bases de données, reportez-vous à *Matrices de compatibilité vSphere*.

Limitation de la connectivité réseau vCenter Server

Pour plus de sécurité, évitez d'installer le système vCenter Server sur un réseau autre qu'un réseau de gestion et assurez-vous que le trafic de gestion vSphere circule sur un réseau restreint. En limitant la connectivité du réseau, vous limitez l'éventualité de certains types d'attaque.

vCenter Server requiert uniquement l'accès à un réseau de gestion. Évitez de placer le système vCenter Server sur d'autres réseaux tels que vos réseaux de production ou de stockage, ou sur tout réseau ayant accès à Internet. vCenter Server n'a pas besoin d'un accès au réseau sur lequel vMotion fonctionne.

vCenter Server requiert une connectivité réseau vers les systèmes suivants.

- Tous les hôtes ESXi.
- La base de données vCenter Server.
- D'autres systèmes vCenter Server (si les systèmes vCenter Server appartiennent à un domaine vCenter Single Sign-On commun, à des fins de réplication des balises, des autorisations, etc.)
- Des systèmes autorisés à exécuter des clients de gestion. Par exemple, vSphere Web Client, un système Windows sous lequel vous utilisez PowerCLI ou tout autre client SDK.
- Des systèmes qui exécutent des composants complémentaires, tels que VMware vSphere Update Manager.
- Des services d'infrastructure, tels que DNS, Active Directory et NTP.
- D'autres systèmes qui exécutent des composants essentiels à la fonctionnalité du système vCenter Server.

Utilisez un pare-feu local sur le système Windows sur lequel le système vCenter Server s'exécute ou utilisez un pare-feu de réseau. Incluez des restrictions d'accès basées sur l'IP, afin que seuls les composants nécessaires puissent communiquer avec le système vCenter Server.

Évaluer l'utilisation de clients Linux avec des interfaces de lignes de commande et des SDK

Les communications entre les composants clients et un système vCenter Server ou des hôtes ESXi sont protégées par défaut par un chiffrement SSL. Les versions Linux de ces composants n'effectuent pas de validation de certificats. Envisagez de restreindre l'utilisation de ces clients.

Même si vous avez remplacé les certificats signés par VMCA sur le système vCenter Server et sur les hôtes ESXi par des certificats qui sont signés par une autorité de certification tierce, certaines communications avec les clients Linux sont toujours vulnérables aux attaques de l'intercepteur. Les composants suivants sont vulnérables lorsqu'ils fonctionnent sur le système d'exploitation Linux.

- Commandes vCLI
- Scripts vSphere SDK for Perl
- Programmes écrits à l'aide de vSphere Web Services SDK

Vous pouvez assouplir la restriction de l'utilisation des clients Linux à condition d'assurer un contrôle adéquat.

- Limitez l'accès au réseau de gestion exclusivement aux systèmes autorisés.
- Utilisez des pare-feux pour vous assurer que seuls les hôtes autorisés peuvent accéder à vCenter Server.
- Utilisez les systèmes JumpBox afin de vous assurer que les clients Linux se trouvent derrière le saut.

Vérifier les plug-in installés

Les extensions vSphere Web Client sont exécutées avec le même niveau de privilège que l'utilisateur qui est connecté. Une extension malveillante peut se faire passer pour un plug-in utile et effectuer des opérations nuisibles, notamment le vol d'informations d'identification ou la modification de la configuration système. Pour augmenter la sécurité, utilisez une installation vSphere Web Client qui comporte uniquement des extensions autorisées provenant de sources fiables.

Une installation vCenter comprend l'infrastructure d'extensibilité vSphere Web Client qui offre la possibilité d'étendre vSphere Web Client à l'aide de sélections de menu ou d'icônes de la barre d'outils qui donnent accès aux composants complémentaires de vCenter ou à des fonctionnalités Web externes. Cette flexibilité s'accompagne du risque d'introduire des fonctionnalités non souhaitées. Par exemple, si un administrateur installe un plug-in dans une instance de vSphere Web Client, le plug-in peut alors exécuter des commandes arbitraires grâce au niveau de privilège de cet administrateur.

Pour protéger votre vSphere Web Client de tout risque éventuel, vous pouvez examiner périodiquement tous les plug-ins installés et vous assurer qu'ils proviennent d'une source fiable.

Prérequis

Vous devez disposer de privilèges pour accéder au service vCenter Single Sign-On. Ces privilèges diffèrent des privilèges vCenter Server.

Procédure

1 Connectez-vous à vSphere Web Client en tant qu'administrator@vsphere.local ou utilisateur avec des privilèges vCenter Single Sign-On.

2 Sur la page d'accueil, sélectionnez **Administration**, puis **Plug-ins des clients** dans **Solutions**

3 Examinez la liste de plug-ins des clients.

Meilleures pratiques de sécurité de vCenter Server Appliance

Suivez toutes les meilleures pratiques de sécurisation d'un système vCenter Server pour sécuriser vCenter Server Appliance. Des procédures supplémentaires vous permettent de renforcer la sécurité de votre dispositif.

Configurer NTP

Assurez-vous que tous les systèmes utilisent la même source de temps relatif. Cette source de temps doit être en synchronisation avec une norme de temps convenue, comme par exemple UTC (temps universel coordonné). La synchronisation des systèmes est essentielle pour la validation des certificats. NTP simplifie également le suivi d'un éventuel intrus dans les fichiers journaux. Des réglages d'heure incorrects compliquent l'analyse et la corrélation de fichiers journaux pour détecter d'éventuelles attaques et compromettent la précision des audits. Reportez-vous à « Synchroniser l'heure dans vCenter Server Appliance avec un serveur NTP », page 188.

Limiter l'accès au réseau de vCenter Server Appliance

Limitez l'accès aux composants qui sont nécessaires pour communiquer avec le dispositif vCenter Server Appliance. En bloquant l'accès des systèmes non essentiels, vous réduisez les risques d'attaque sur le système d'exploitation. Reportez-vous aux sections « Ports requis pour vCenter Server et l'instance de Platform Services Controller », page 114 et « Ports TCP et UDP supplémentaires pour vCenter Server », page 119. Pour configurer votre environnement avec des paramètres de pare-feu compatibles avec le STIG DISA, suivez les directives de l'article 2047585 dans la base de connaissances VMware.

Exigences de mots de passe et comportement de verrouillage de vCenter

Pour gérer votre environnement vSphere, vous devez connaître la stratégie de mot de passe vCenter Single Sign-On, les mots de passe vCenter Server et le comportement de verrouillage.

Cette section traite des mots de passe vCenter Single Sign-On. Reportez-vous à « Verrouillage des mots de passe et des comptes ESXi », page 45 pour une description des mots de passe des utilisateurs locaux d'ESXi.

Mot de passe d'administrateur vCenter Single Sign-On

Le mot de passe de l'administrateur de vCenter Single Sign-On, administrator@vsphere.local par défaut, est spécifié par la stratégie de mot de passe de vCenter Single Sign-On. Par défaut, ce mot de passe doit répondre aux exigences suivantes.

- Au moins 8 caractères
- Au moins un caractère minuscule
- Au moins un caractère numérique
- Au moins un caractère spécial

Le mot de passe de cet utilisateur ne peut pas dépasser 20 caractères. À partir de vSphere 6.0, les caractères non ASCII sont autorisés. Les administrateurs peuvent modifier la stratégie de mot de passe par défaut. Consultez la documentation de *Administration de Platform Services Controller* .

Mots de passe d' vCenter Server

Dans vCenter Server, les exigences en matière de mot de passe sont dictées par vCenter Single Sign-On ou par la source d'identité configurée qui peut être Active Directory ou OpenLDAP.

Comportement de verrouillage de vCenter Single Sign-On

Les utilisateurs sont verrouillés après un nombre prédéfini de tentatives de connexion infructueuses successives. Par défaut, les utilisateurs sont verrouillés après cinq tentatives infructueuses successives en trois minutes et un compte verrouillé est déverrouillé automatiquement après cinq minutes. Vous pouvez modifier ces valeurs par défaut à l'aide de la stratégie de verrouillage de vCenter Single Sign-On. Consultez la documentation de *Administration de Platform Services Controller* .

À partir de vSphere 6.0, l'administrateur du domaine vCenter Single Sign-On, administrator@vsphere.local par défaut, n'est pas affecté par la stratégie de verrouillage. L'utilisateur est affecté par la stratégie de mot de passe.

Modifications du mot de passe

Si vous connaissez votre mot de passe, vous pouvez le modifier à l'aide de la commande `dir-cli password change`. Si vous avez oublié votre mot de passe, un administrateur vCenter Single Sign-On peut le réinitialiser à l'aide de la commande `dir-cli password reset`.

Pour obtenir des informations sur l'expiration du mot de passe et d'autres rubriques associés dans différentes versions de vSphere, reportez-vous à la base de connaissances VMware.

Vérifier les empreintes des hôtes ESXi hérités

Dans vSphere 6 et versions ultérieures, des certificats VMCA sont attribués aux hôtes par défaut. Si vous passez au mode de certificat d'empreinte, vous pouvez continuer à utiliser le mode d'empreinte pour les hôtes hérités. Vous pouvez vérifier les empreintes dans vSphere Web Client.

Remarque Les certificats sont conservés par défaut entre les mises à niveau.

Procédure

1 Accédez au système vCenter Server dans le navigateur d'objets de vSphere Web Client.

2 Cliquez sur **Configurer**.

3 Sous **Paramètres**, cliquez sur **Général**

4 Cliquez sur **Modifier**.

5 Cliquez sur **Paramètres SSL**.

6 Si l'un de vos hôtes ESXi 5.5 ou version antérieure nécessite une validation manuelle, comparez les empreintes répertoriées pour les hôtes aux empreintes de la console hôte.

   Pour obtenir l'empreinte de l'hôte, utilisez l'interface utilisateur de console directe (DCUI).

   a Connectez-vous à la console directe et appuyez sur F2 pour accéder au menu de Personnalisation du système.

   b Sélectionnez **Voir les informations de support**.

      L'empreinte hôte figure dans la colonne de droite.

7 Si l'empreinte correspond, cochez la case **Vérifier** à côté de l'hôte.

   Les hôtes non sélectionnés sont déconnectés après avoir cliqué sur **OK**.

8 Cliquez sur **OK**.

Vérifier que la validation des certificats SSL sur Network File Copy est activée

La NFC (Network File Copy, copie de fichiers réseau) fournit un service FTP capable de reconnaître les types de fichiers pour les composants vSphere. À partir de vSphere 5.5, ESXi utilise par défaut NFC pour les opérations telles que la copie et le déplacement de données entre les banques de données, mais si la fonction est désactivée, vous devrez l'activer.

Lorsque SSL sur NFC est activé, les connexions entre les composants de vSphere via le protocole NFC sont sécurisées. Cette connexion permet d'éviter des « attaques de l'intercepteur » au sein d'un centre de données.

Dans la mesure où l'utilisation de NFC via SSL entraîne une dégradation des performances, vous pouvez envisager de désactiver ce paramètre avancé dans certains environnements de développement.

Remarque Définissez explicitement cette valeur sur true si vous utilisez des scripts pour vérifier la valeur.

Procédure

1 Connectez-vous à vCenter Server avec vSphere Web Client.

2 Cliquez sur **Configurer**.

3 Cliquez sur **Paramètres avancés** et saisissez la clé et la valeur suivantes en bas de la boîte de dialogue.

Champ	Valeur
Touche	config.nfc.useSSL
Valeur	vrai

4 Cliquez sur **OK**.

Ports requis pour vCenter Server et l'instance de Platform Services Controller

Le système vCenter Server, sur Windows et sur le dispositif, doit pouvoir envoyer des données à chaque hôte géré et recevoir des données de vSphere Web Client et des services Platform Services Controller. Pour autoriser les activités de migration et de provisionnement entre les hôtes gérés, les hôtes source et destination doivent pouvoir recevoir des données l'un de l'autre.

Si un port est en cours d'utilisation ou est inscrit sur la liste noire, le programme d'installation de vCenter Server affiche un message d'erreur. Vous devez utiliser un autre numéro de port pour poursuivre l'installation. Des ports internes sont utilisés uniquement pour la communication entre processus.

VMware utilise des ports désignés pour la communication. En outre, les hôtes gérés surveillent des ports désignés pour détecter l'arrivée de données en provenance de vCenter Server. Si un pare-feu intégré existe entre ces éléments, le programme d'installation ouvre les ports pendant le processus d'installation ou de mise à niveau. Pour les pare-feu personnalisés, vous devez ouvrir les ports requis. Si vous avez un pare-feu entre deux hôtes gérés et que vous désirez effectuer des activités source ou cible, comme une migration ou un clonage, vous devez configurer un moyen pour que les hôtes gérés puissent recevoir des données.

Remarque Dans Microsoft Windows Server 2008 et versions ultérieures, le pare-feu est activé par défaut.

Tableau 4-1. Ports requis pour la communication entre les composants

Port	Protocole	Description	Requis pour	Utilisé pour la communication nœud à nœud
22	TCP/UDP	Port système de SSHD.	Déploiements de dispositifs de ■ vCenter Server ■ Platform Services Controller	Non
80	TCP	vCenter Server nécessite le port 80 pour les connexions HTTP directes. Le port 80 redirige les requêtes vers le port 443 HTTPS. Cette redirection est utile si vous utilisez accidentellement http://serveur au lieu de https://serveur. WS-Management (nécessite également l'ouverture du port 443). Si vous utilisez une base de données Microsoft SQL qui est stockée sur la même machine virtuelle ou le même serveur physique que vCenter Server, le port 80 est utilisé par SQL Reporting Service. Lorsque vous installez ou mettez à niveau vCenter Server, le programme d'installation vous invite à modifier le port HTTP pour vCenter Server. Modifiez le port HTTP vCenter Server à une valeur personnalisée pour garantir la réussite de l'installation ou de la mise à niveau. **Important** Vous pouvez modifier ce numéro de port pendant les installations de vCenter Server et de Platform Services Controller sous Windows.	Installations Windows et déploiement de dispositifs de ■ vCenter Server ■ Platform Services Controller	Non
88	TCP	Serveur Active Directory.	Installations Windows et déploiement de dispositifs de Platform Services Controller	Non
389	TCP/UDP	Ce port doit être ouvert sur les instances locales et distantes de vCenter Server. Il s'agit du numéro de port LDAP des services d'annuaire du groupe vCenter Server. Si un autre service utilise ce port, il est préférable de le supprimer ou de lui attribuer un autre port. Vous pouvez faire fonctionner le service LDAP sur n'importe quel autre port entre 1025 et 65535. Si cette instance sert de Microsoft Windows Active Directory, modifiez le numéro de port 389 pour un numéro de port disponible entre 1025 et 65535.	Installations Windows et déploiement de dispositifs de Platform Services Controller	■ vCenter Server vers Platform Services Controller ■ Platform Services Controller vers Platform Services Controller

Tableau 4-1. Ports requis pour la communication entre les composants (suite)

Port	Protocole	Description	Requis pour	Utilisé pour la communication nœud à nœud
443	TCP	Port par défaut que le système vCenter Server utilise pour écouter les connexions provenant de vSphere Web Client. Pour autoriser le système vCenter Server à recevoir des données de vSphere Web Client, ouvrez le port 443 dans le pare-feu. Le système vCenter Server utilise également le port 443 pour surveiller les transferts de données depuis les clients SDK. Ce port est également utilisé pour les services suivants : ■ WS-Management (nécessite également l'ouverture du port 80) ■ Connexions clients de gestion de réseau tiers à vCenter Server ■ Accès clients de gestion de réseau tiers à des hôtes **Important** Vous pouvez modifier ce numéro de port pendant les installations de vCenter Server et de Platform Services Controller sous Windows.	Installations Windows et déploiement de dispositifs de ■ vCenter Server ■ Platform Services Controller	■ vCenter Server vers vCenter Server ■ vCenter Server vers Platform Services Controller ■ Platform Services Controller vers vCenter Server
514	UDP	Port vSphere Syslog Collector pour vCenter Server sur Windows et port vSphere Syslog Service pour vCenter Server Appliance **Important** Vous pouvez modifier ce numéro de port pendant les installations de vCenter Server et de Platform Services Controller sous Windows.	Installations Windows et déploiement de dispositifs de ■ vCenter Server ■ Platform Services Controller	Non
636	TCP	vCenter Single Sign-On LDAPS	-	Pour une compatibilité descendante avec vSphere 6.0 uniquement. vCenter Server 6.0 vers Platform Services Controller 6.5

Tableau 4-1. Ports requis pour la communication entre les composants (suite)

Port	Protocole	Description	Requis pour	Utilisé pour la communication nœud à nœud
902	TCP/UDP	Le port par défaut utilisé par vCenter Server pour envoyer des données à des hôtes gérés. Les hôtes gérés envoient également régulièrement un signal de pulsation par le port UDP 902 au système vCenter Server. Ce port ne doit pas être bloqué par les pare-feu entre le serveur et les hôtes, ou entre les hôtes. Le port 902 ne doit pas être bloqué entre le VMware Host Client et les hôtes. Le VMware Host Client utilise ce port pour afficher les consoles des machines virtuelles. **Important** Vous pouvez modifier ce numéro de port pendant les installations de vCenter Server sous Windows.	Installations Windows et déploiement de dispositifs de vCenter Server	Non
1514	TCP/UDP	Port vSphere Syslog Collector TLS pour vCenter Server sur Windows et port vSphere Syslog Service TLS pour vCenter Server Appliance **Important** Vous pouvez modifier ce numéro de port pendant les installations de vCenter Server et de Platform Services Controller sous Windows.	Installations Windows et déploiement de dispositifs de ■ vCenter Server ■ Platform Services Controller	Non
2012	TCP	Interfaces de contrôle RPC pour vCenter Single Sign-On	Installations Windows et déploiement de dispositifs de Platform Services Controller	■ vCenter Server vers Platform Services Controller ■ Platform Services Controller vers vCenter Server ■ Platform Services Controller vers Platform Services Controller
2014	TCP	Port RPC pour toutes les API VMCA (VMware Certificate Authority) **Important** Vous pouvez modifier ce numéro de port pendant les installations de Platform Services Controller sous Windows.	Installations Windows et déploiement de dispositifs de Platform Services Controller	■ vCenter Server vers Platform Services Controller ■ Platform Services Controller vers vCenter Server
2020	TCP/UDP	Gestion de la structure d'authentification **Important** Vous pouvez modifier ce numéro de port pendant les installations de vCenter Server et de Platform Services Controller sous Windows.	Installations Windows et déploiement de dispositifs de ■ vCenter Server ■ Platform Services Controller	■ vCenter Server vers Platform Services Controller ■ Platform Services Controller vers vCenter Server

Tableau 4-1. Ports requis pour la communication entre les composants (suite)

Port	Protocole	Description	Requis pour	Utilisé pour la communication nœud à nœud
6500	TCP/UDP	port d'ESXi Dump Collector **Important** Vous pouvez modifier ce numéro de port pendant les installations de vCenter Server sous Windows.	Installations Windows et déploiement de dispositifs de vCenter Server	Non
6501	TCP	Service Auto Deploy **Important** Vous pouvez modifier ce numéro de port pendant les installations de vCenter Server sous Windows.	Installations Windows et déploiement de dispositifs de vCenter Server	Non
6502	TCP	Gestion Auto Deploy **Important** Vous pouvez modifier ce numéro de port pendant les installations de vCenter Server sous Windows.	Installations Windows et déploiement de dispositifs de vCenter Server	Non
7444	TCP	Service de jeton sécurisé	Installations Windows et déploiement de dispositifs de Platform Services Controller	■ vCenter Server vers Platform Services Controller ■ Platform Services Controller vers vCenter Server
9123	TCP	Port de l'assistant de migration	Installations Windows et déploiement de dispositifs de vCenter Server	Instance source de vCenter Server ou vCenter Single Sign-On vers l'instance cible de vCenter Server Appliance ou Platform Services Controller
9443	TCP	vSphere Web Client HTTPS	Installations Windows et déploiement de dispositifs de vCenter Server	Non
11711	TCP	vCenter Single Sign-On LDAP	-	Pour une compatibilité descendante avec vSphere 5.5 uniquement. vCenter Single Sign-On 5.5 vers Platform Services Controller 6.5
11712	TCP	vCenter Single Sign-On LDAPS	-	Pour une compatibilité descendante avec vSphere 5.5 uniquement. vCenter Single Sign-On 5.5 vers Platform Services Controller 6.5

Pour configurer le système vCenter Server de manière à utiliser un autre port pour recevoir les données de vSphere Web Client, reportez-vous à la documentation *Gestion de vCenter Server et des hôtes*.

Pour plus d'informations sur la configuration du pare-feu, reportez-vous à la documentation *Sécurité vSphere*.

Ports TCP et UDP supplémentaires pour vCenter Server

vCenter Server est accessible par le biais de ports TCP et UDP prédéterminés. Si vous gérez des composants réseau à partir de l'extérieur d'un pare-feu, vous pouvez être invité à reconfigurer le pare-feu pour autoriser l'accès sur les ports appropriés.

« Ports requis pour vCenter Server et l'instance de Platform Services Controller », page 114 donne la liste des ports qui sont ouverts par l'installateur dans le cadre d'une installation par défaut. Certains ports supplémentaires sont requis pour certains services, tels que NTP, ou des applications qui sont généralement installées avec vCenter Server.

En plus de ces ports, vous pouvez configurer d'autres ports en fonction de vos besoins.

Tableau 4-2. Ports TCP et UDP pour vCenter Server

Port	Protocole	Description
123 (UDP)	UDP	Client NTP. Si vous déployez vCenter Server Appliance dans un hôte ESXi, la date/heure de ces deux éléments doit être synchronisée, le plus souvent au moyen d'un serveur NTP, et le port correspondant doit être ouvert.
135	TCP	Pour vCenter Server Appliance, ce port est désigné pour l'authentification Active Directory. Pour une installation de vCenter Server sur Windows, ce port est utilisé pour Linked mode et le port 88 est utilisé pour l'authentification Active Directory.
161	UDP	Serveur SNMP.
636	TCP	vCenter Single Sign-On LDAPS (6.0 et ultérieur)
8084, 9084, 9087	TCP	Utilisé par vSphere Update Manager
8109	TCP	VMware Syslog Collector. Ce service est nécessaire pour centraliser la collecte.
15007, 15008	TCP	vService Manager (VSM). Ce service enregistre les extensions de vCenter Server. Ouvrez ce port uniquement si cela est requis par les extensions que vous prévoyez d'utiliser.
31031, 44046 (par défaut)	TCP	vSphere Replication.

Les ports suivants sont utilisés exclusivement en interne.

Tableau 4-3. Ports TCP et UDP pour vCenter Server

Port	Description
5443	Port interne de l'interface utilisateur graphique de vCenter Server.
5444, 5432	Port interne de surveillance de vPostgreSQL.
5090	Port interne de l'interface utilisateur graphique de vCenter Server.
7080	Port interne de service de jetons sécurisés.
7081	Port interne de Platform Services Controller.
8000	Port interne pour ESXi Dump Collector.
8006	Utilisé pour la surveillance de l'état de santé de Virtual SAN.

Tableau 4-3. Ports TCP et UDP pour vCenter Server (suite)

Port	Description
8085	Ports internes utilisés par le SDK du service vCenter (vpxd).
8095	Port du flux de services VMware vCenter.
8098, 8099	Utilisé par VMware Image Builder Manager.
8190, 8191, 22000, 22100, 21100	VMware vSphere Profile-Driven Storage Service
8200, 8201, 5480	Ports internes de gestion des dispositifs.
8300, 8301	Ports réservés de gestion des dispositifs.
8900	Port interne de surveillance d'API.
9090	Port interne de vSphere Web Client.
10080	Port interne du service d'inventaire
10201	Port interne du service de configuration du bus de messages.
11080	Ports internes de vCenter Server Appliance pour HTTP et l'écran de présentation.
12721	Port interne de service de jetons sécurisés.
12080	Port interne du service de licence.
12346, 12347, 4298	Port interne pour les SDK de VMware Cloud Management (vAPI)
13080, 6070	Utilisation interne par le service Performance Charts.
14080	Utilisation interne par le service Syslog.
15005, 15006	Port interne d'ESX Agent Manager.
16666, 16667	Ports du service Content Library.
18090	Port interne de Content Manager.
18091	Port interne de Component Manager.

Sécurisation des machines virtuelles 5

Le système d'exploitation client qui est exécuté dans la machine virtuelle est exposé aux mêmes risques de sécutité qu'une machine physique. Sécurisez les machines virtuelles de la même manière que les machines physiques, et suivez les meilleures pratiques présentées dans ce document et dans le *Guide de sécurisation renforcée*.

Ce chapitre aborde les rubriques suivantes :

Activer ou désactiver le démarrage sécurisé UEFI pour une machine virtuelle

Le démarrage sécurisé UEFI est une norme de sécurité qui permet de vérifier que votre ordinateur démarre uniquement avec les logiciels approuvés par le fabricant. Pour certaines versions matérielles et certains systèmes d'exploitation de machines virtuelles, vous pouvez activer le démarrage sécurisé de la même manière que pour une machine physique.

Dans un système d'exploitation qui prend en charge le démarrage sécurisé UEFI, chaque logiciel de démarrage est signé, notamment le chargeur de démarrage, le noyau du système d'exploitation et les pilotes du système d'exploitation. La configuration par défaut de la machine virtuelle inclut plusieurs certificats de signature de code.

- Un certificat Microsoft utilisé uniquement pour démarrer Windows.
- Un certificat Microsoft utilisé pour le code tiers qui est signé par Microsoft, comme les chargeurs de démarrage Linux.
- Un certificat VMware qui est utilisé uniquement pour démarrer ESXi dans une machine virtuelle.

La configuration par défaut de la machine virtuelle inclut un certificat pour authentifier les demandes de modification de la configuration du démarrage sécurisé, notamment la liste de révocation de démarrage sécurisé, depuis la machine virtuelle, qui est un certificat Microsoft KEK (Key Exchange Key).

Dans la plupart des cas, il n'est pas nécessaire de remplacer les certificats existants. Si vous souhaitez remplacer les certificats, reportez-vous au système de la base de connaissances VMware.

La version 10.1 ou ultérieure de VMware Tools est requise pour les machines virtuelles qui utilisent le démarrage sécurisé UEFI. Vous pouvez mettre à niveau ces machines virtuelles vers une version ultérieure de VMware Tools, le cas échéant.

Pour les machines virtuelles Linux, VMware Host-Guest Filesystem n'est pas pris en charge en mode de démarrage sécurisé. Supprimez VMware Host-Guest Filesystem de VMware Tools avant d'activer le démarrage sécurisé.

Remarque Si vous activez le démarrage sécurisé pour une machine virtuelle, vous ne pouvez charger que des pilotes signés sur cette machine virtuelle.

Prérequis

Vous pouvez activer le démarrage sécurisé uniquement si toutes les conditions préalables sont remplies. Si les conditions préalables ne sont pas remplies, la case à cocher n'est pas visible dans vSphere Web Client.

- Vérifiez que le système d'exploitation et le micrologiciel de la machine virtuelle prennent en charge le démarrage UEFI.
  - Micrologiciel EFI
  - Matériel virtuel version 13 ou ultérieure.
  - Système d'exploitation prenant en charge le démarrage sécurisé UEFI. Reportez-vous au *Guide de compatibilité VMware* pour obtenir des informations actualisées.

  Remarque Vous ne pouvez pas mettre à niveau une machine virtuelle qui utilise le démarrage BIOS vers une machine virtuelle qui utilise le démarrage UEFI. Si vous mettez à niveau une machine virtuelle qui utilise déjà le démarrage UEFI vers un système d'exploitation prenant en charge le démarrage sécurisé UEFI, vous pouvez activer le démarrage sécurisé pour cette machine virtuelle.
- Désactivez la machine virtuelle. Si la machine virtuelle est en cours d'exécution, la case est grisée.

Vous devez disposer de privilèges **VirtualMachine.Config.Settings** pour activer ou désactiver le démarrage sécurisé UEFI pour la machine virtuelle.

Procédure

1 Connectez-vous à vSphere Web Client, puis sélectionnez la machine virtuelle.

2 Dans la boîte de dialogue **Modifier les paramètres**, ouvrez **Options de démarrage** et vérifiez que le micrologiciel est défini sur **EFI**.

3 Cochez la case **Activer le démarrage sécurisé**, puis cliquez sur **OK**.

4 Si, par la suite, vous souhaitez désactiver le démarrage sécurisé, cliquez de nouveau sur la case.

Lorsque la machine virtuelle démarre, seuls les composants ayant des signatures valides sont autorisés. Le processus de démarrage s'arrête avec une erreur s'il rencontre un composant ayant une signature manquante ou non valide.

Limiter les messages d'information des machines virtuelles vers les fichiers VMX

Limitez les messages d'information de la machine virtuelle vers le fichier VMX, afin d'éviter de remplir la banque de données et de causer un déni de service (DoS). Un déni de service peut survenir quand vous ne contrôlez pas la taille du fichier VMX d'une machine virtuelle et que la quantité d'informations excède la capacité de la banque de données.

La limite par défaut du fichier de configuration de machine virtuelle (fichier VMX) est de 1 Mo. Cette capacité est généralement insuffisante, mais vous pouvez modifier cette valeur si nécessaire. Par exemple, vous pouvez augmenter la limite si vous stockez des quantités importantes d'informations personnalisées dans le fichier.

Remarque Étudiez soigneusement le volume d'informations dont vous avez besoin. Si la quantité d'informations excède la capacité de la banque de données, un déni de service peut survenir.

La limite par défaut de 1 Mo s'applique même si le paramètre `tools.setInfo.sizeLimit` n'est pas répertorié dans les options avancées.

Procédure

1 Connectez-vous à un système vCenter Server à l'aide de vSphere Web Client et localisez la machine virtuelle.

   a Dans le navigateur, sélectionnez **VM et modèles**.

   b Localisez la machine virtuelle dans la hiérarchie.

2 Cliquez avec le bouton droit sur la machine virtuelle et cliquez sur**Modifier les paramètres**.

3 Sélectionnez **Options VM**.

4 Cliquez sur **Avancées**, puis cliquez sur **Modifier la configuration**.

5 Ajoutez ou modifiez le paramètre `tools.setInfo.sizeLimit`.

Empêcher la réduction de disque virtuel

Les utilisateurs non administratifs du système d'exploitation client peuvent réduire les disques virtuels. La réduction d'un disque virtuel exige de l'espace inutilisé sur le disque. Cependant, si vous réduisez un disque virtuel de façon répétée, le disque peut devenir indisponible et provoquer un déni de service. Pour éviter cela, désactivez la possibilité de réduction des disques virtuels.

Prérequis

- Désactivez la machine virtuelle.
- Vérifiez que vous disposez des privilèges racine ou d'administrateur sur la machine virtuelle.

Procédure

1 Connectez-vous à un système vCenter Server à l'aide de vSphere Web Client et localisez la machine virtuelle.

   a Dans le navigateur, sélectionnez **VM et modèles**.

   b Localisez la machine virtuelle dans la hiérarchie.

2 Cliquez avec le bouton droit sur la machine virtuelle et cliquez sur**Modifier les paramètres**.

3 Sélectionnez **Options VM**.

4 Cliquez sur **Avancées**, puis cliquez sur **Modifier la configuration**.

5 Ajoutez ou modifiez les paramètres suivants.

Nom	Valeur
isolation.tools.diskWiper.disable	TRUE
isolation.tools.diskShrink.disable	TRUE

6 Cliquez sur **OK**.

Lorsque vous désactivez cette fonction, vous ne pouvez plus réduire des disques de machines virtuelles lorsqu'une banque de données vient à manquer d'espace.

Recommandations en matière de sécurité des machines virtuelles

Suivez les recommandations suivantes pour garantir l'intégrité de votre déploiement vSphere.

- Protection générale d'une machine virtuelle page 124

  Une machine virtuelle est, pour l'essentiel, l'équivalent d'un serveur physique. Il convient de prendre les mêmes mesures de sécurité pour les machines virtuelles et les systèmes physiques.

- Utiliser des modèles pour déployer des machines virtuelles page 125

  Lorsque vous installez manuellement des systèmes d'exploitation clients et des applications sur une machine virtuelle, le risque existe que votre configuration soit incorrecte. Grâce à l'utilisation d'un modèle pour capturer une image sécurisée du système d'exploitation de base sans applications installées, vous pouvez vous assurer que toutes les machines virtuelles sont créées avec une ligne de base connue du niveau de sécurité.

- Minimiser l'utilisation de la console de machine virtuelle page 125

  La console de machine virtuelle joue pour la machine virtuelle le même rôle qu'un moniteur sur un serveur physique. Les utilisateurs qui ont accès à la console de machine virtuelle ont accès à la gestion de l'alimentation des machines virtuelles et aux contrôles de la connectivité des périphériques amovibles. L'accès à la console peut donc permettre une attaque malveillante sur une machine virtuelle.

- Empêcher les machines virtuelles de récupérer les ressources page 126

  Lorsqu'une machine virtuelle consomme une telle proportion des ressources de l'hôte que les autres machines virtuelles de l'hôte ne peuvent accomplir les fonctions pour lesquelles elles sont prévues, un déni de service (DoS) peut survenir. Pour empêcher une machine virtuelle de provoquer un DoS, utilisez les fonctions de gestion des ressources de l'hôte, telles que le paramétrage des partages, et utilisez des pools de ressources.

- Désactiver les fonctions inutiles à l'intérieur des machines virtuelles page 126

  Tout service exécuté sur une machine virtuelle peut entraîner l'attaque de cette dernière. En désactivant les composants du système qui ne sont pas nécessaires pour prendre en charge l'application ou le service exécuté sur le système, vous réduisez les risques d'attaque.

Protection générale d'une machine virtuelle

Une machine virtuelle est, pour l'essentiel, l'équivalent d'un serveur physique. Il convient de prendre les mêmes mesures de sécurité pour les machines virtuelles et les systèmes physiques.

Respectez ces recommandations pour protéger votre machine virtuelle :

Correctifs et autres protections

Maintenez toutes vos mesures de sécurité à jour, y compris en appliquant les correctifs appropriés. Il est tout particulièrement important de ne pas négliger les machines virtuelles dormantes désactivées et de suivre les mises à jour les concernant. Par exemple, assurez-vous que le logiciel antivirus, les produits anti-spyware, la détection d'intrusion et toute autre protection sont activés pour chaque machine virtuelle dans votre infrastructure virtuelle. Vous devez également vous assurer de disposer de suffisamment d'espace pour les journaux des machines virtuelles.

Analyses antivirus

Comme chaque machine virtuelle héberge un système d'exploitation standard, vous devez le protéger des virus en installant antivirus. En fonction de votre utilisation habituelle de la machine virtuelle, vous pouvez installer également un pare-feu.

Planifiez l'exécution de scan de virus, tout particulièrement en cas de déploiement incluant un grand nombre de machines virtuelles. Si vous scannez toutes les machines virtuelles simultanément, les performances des systèmes de votre environnement enregistrent une baisse importante. Les pare-feu et les logiciels anti-virus peuvent exiger une grande quantité de virtualisation ; par conséquent, vous pouvez équilibrer ces deux mesures en fonction des performances souhaitées au niveau des machines virtuelles (et tout particulièrement si vous pensez que vos machines virtuelles se trouvent dans un environnement totalement sécurisé).

Ports série Les ports série sont des interfaces permettant de connecter des périphériques à la machine virtuelle. Ils sont souvent utilisés sur les systèmes physiques pour fournir une connexion directe, de bas niveau à la console d'un serveur. Un port série virtuel autorise le même accès à une machine virtuelle. Les ports série permettent un accès de bas niveau, qui n'offre souvent pas de contrôle renforcé, tel que journalisation ou privilèges.

Utiliser des modèles pour déployer des machines virtuelles

Lorsque vous installez manuellement des systèmes d'exploitation clients et des applications sur une machine virtuelle, le risque existe que votre configuration soit incorrecte. Grâce à l'utilisation d'un modèle pour capturer une image sécurisée du système d'exploitation de base sans applications installées, vous pouvez vous assurer que toutes les machines virtuelles sont créées avec une ligne de base connue du niveau de sécurité.

Vous pouvez utiliser des modèles qui contiennent un système d'exploitation sécurisé doté de correctifs et correctement configuré pour créer d'autres modèles propres à des applications ou utiliser le modèle d'application pour déployer des machines virtuelles.

Procédure

- Fournissez des modèles pour la création de machines virtuelles qui comportent des déploiements de systèmes d'exploitation sécurisés, corrigés et correctement configurés.

  Si possible, déployez également les applications dans les modèles. Assurez-vous que les applications ne dépendent pas d'informations spécifiques à la machine virtuelle à déployer.

Suivant

Pour plus d'informations sur les modèles, reportez-vous à la documentation *Administration d'une machine virtuelle vSphere*.

Minimiser l'utilisation de la console de machine virtuelle

La console de machine virtuelle joue pour la machine virtuelle le même rôle qu'un moniteur sur un serveur physique. Les utilisateurs qui ont accès à la console de machine virtuelle ont accès à la gestion de l'alimentation des machines virtuelles et aux contrôles de la connectivité des périphériques amovibles. L'accès à la console peut donc permettre une attaque malveillante sur une machine virtuelle.

Procédure

1. Utilisez des services natifs de gestion à distance, tels que des services de terminaux et SSH, pour interagir avec les machines virtuelles.

   Autorisez l'accès à la console de machine virtuelle uniquement lorsque cela est nécessaire.

2 Limitez les connexions à la console.

Par exemple, dans un environnement hautement sécurisé, limitez ce nombre à une connexion. Dans certains environnements, vous pouvez augmenter la limite si plusieurs connexions simultanées sont requises pour effectuer des tâches normales.

Empêcher les machines virtuelles de récupérer les ressources

Lorsqu'une machine virtuelle consomme une telle proportion des ressources de l'hôte que les autres machines virtuelles de l'hôte ne peuvent accomplir les fonctions pour lesquelles elles sont prévues, un déni de service (DoS) peut survenir. Pour empêcher une machine virtuelle de provoquer un DoS, utilisez les fonctions de gestion des ressources de l'hôte, telles que le paramétrage des partages, et utilisez des pools de ressources.

Par défaut, toutes les machines virtuelles d'un hôte ESXi partagent équitablement les ressources. Vous pouvez utiliser les partages et les pools de ressources pour empêcher une attaque par déni de service amenant une machine virtuelle à consommer une quantité si importante des ressources de l'hôte que les autres machines virtuelles sur le même hôte ne peuvent pas remplir les fonctions prévues.

N'utilisez pas de limites si vous n'en comprenez pas complètement l'impact.

Procédure

1 Fournissez à chaque machine virtuelle juste ce qu'il faut de ressources (CPU et mémoire) pour fonctionner correctement.

2 Utilisez les partages pour assurer des ressources suffisantes aux machines virtuelles essentielles.

3 Regroupez les machines virtuelles dont les exigences sont identiques dans des pools de ressources.

4 Dans chaque pool de ressources, conservez la configuration par défaut des partages pour veiller à ce que chaque machine virtuelle du pool bénéficie d'à peu près la même priorité face aux ressources.

Avec ce paramètre, une machine virtuelle individuelle ne peut pas utiliser plus de ressources que les autres machines virtuelles du pool de ressources.

Suivant

Consultez la documentation *Gestion des ressources vSphere* pour de plus amples informations sur les partages et les limites.

Désactiver les fonctions inutiles à l'intérieur des machines virtuelles

Tout service exécuté sur une machine virtuelle peut entraîner l'attaque de cette dernière. En désactivant les composants du système qui ne sont pas nécessaires pour prendre en charge l'application ou le service exécuté sur le système, vous réduisez les risques d'attaque.

En règle générale, les machines virtuelles n'exigent pas autant de services et de fonctions que les serveurs physiques. Lorsque vous virtualisez un système, évaluez si une fonction ou un service est nécessaire.

Procédure

- Désactivez les services inutilisés dans le système d'exploitation.

  Par exemple, si le système exécute un serveur de fichiers, désactivez tous les services Web.

- Déconnectez les périphériques physiques inutilisés, tels que les lecteurs de CD/DVD, les lecteurs de disquettes et les adaptateurs USB.

- Désactivez toute fonctionnalité inutilisée (par exemple, les fonctionnalités d'affichage inutilisées ou HGFS (Host Guest File System)).

- Désactivez les écrans de veille.

- N'exécutez pas le système X Window sous des systèmes d'exploitation invités Linux, BSD ou Solaris, à moins que ce ne soit nécessaire.

Supprimer les périphériques matériels inutiles

Tout périphérique activé ou connecté représente un canal d'attaque potentiel. Les utilisateurs et les processus disposant de privilèges sur une machine virtuelle peuvent connecter ou déconnecter des périphériques matériels (adaptateurs réseau et lecteurs de CD-ROM, par exemple). Les agresseurs peuvent utiliser ce moyen pour déjouer la sécurité des machines virtuelles. La suppression des périphériques matériels inutiles peut aider à la prévention des attaques.

Un pirate ayant accès à une machine virtuelle peut connecter un périphérique matériel déconnecté et accéder à des informations sensibles sur n'importe quel média qui est laissé dans celui-ci. Il peut également déconnecter une carte réseau pour isoler la machine virtuelle de son réseau, ce qui constitue un déni de service.

- Ne connectez pas des périphériques non autorisés à la machine virtuelle.
- Retirez les périphériques matériels inutiles ou inutilisés.
- Désactivez les périphériques virtuels inutiles au sein d'une machine virtuelle.
- Vérifiez que seuls les périphériques requis sont connectés à une machine virtuelle. Les machines virtuelles utilisent rarement les ports série ou parallèles. Les lecteurs de CD/DVD ne sont généralement connectés que temporairement lors de l'installation de logiciels.

Procédure

1 Ouvrez une session sur un système vCenter Server au moyen de vSphere Web Client.

2 Cliquez avec le bouton droit sur la machine virtuelle et cliquez sur**Modifier les paramètres**.

3 Désactivez les périphériques matériels qui ne sont pas nécessaires.

   Vérifiez notamment les périphériques suivants :

   - Lecteurs de disquettes
   - Ports série
   - Ports parallèles
   - contrôleurs USB
   - lecteurs de CD-ROM

Désactiver les fonctionnalités d'affichage inutilisées

Les pirates peuvent utiliser une fonctionnalité d'affichage inutilisée comme vecteur d'insertion de code malveillant dans votre environnement. Désactivez les fonctionnalités qui ne sont pas utilisées dans votre environnement.

Procédure

1 Connectez-vous à un système vCenter Server à l'aide de vSphere Web Client et localisez la machine virtuelle.

   a Dans le navigateur, sélectionnez **VM et modèles**.

   b Localisez la machine virtuelle dans la hiérarchie.

2 Cliquez avec le bouton droit sur la machine virtuelle et cliquez sur**Modifier les paramètres**.

3 Sélectionnez **Options VM**.

4 Cliquez sur **Avancées**, puis cliquez sur **Modifier la configuration**.

5 Le cas échéant, ajoutez ou modifiez les paramètres suivants.

Option	Description
svga.vgaonly	Si vous définissez ce paramètre sur TRUE, les fonctions graphiques avancées ne fonctionnent plus. Seul le mode de console en cellule de caractère sera disponible. Si vous utilisez ce paramètre, `mks.enable3d` n'a aucun effet. **Remarque** Appliquez ce paramètre uniquement aux machines virtuelles n'ayant pas besoin d'une carte vidéo virtualisée.
mks.enable3d	Définissez ce paramètre sur FALSE sur les machines virtuelles n'ayant pas besoin d'une fonctionnalité 3D.

Désactiver les fonctions non exposées

Les machines virtuelles VMware peuvent fonctionner dans un environnement vSphere et sur des plates-formes de virtualisation hébergées comme VMware Workstation et VMware Fusion. Certains paramètres de machine virtuelle ne nécessitent pas d'être activés lorsque vous exécutez une machine virtuelle dans un environnement vSphere. Désactivez ces paramètres afin de réduire les possibilités de vulnérabilités.

Prérequis

Désactivez la machine virtuelle.

Procédure

1 Connectez-vous à un système vCenter Server à l'aide de vSphere Web Client et localisez la machine virtuelle.

   a Dans le navigateur, sélectionnez **VM et modèles**.

   b Localisez la machine virtuelle dans la hiérarchie.

2 Cliquez avec le bouton droit sur la machine virtuelle et cliquez sur**Modifier les paramètres**.

3 Sélectionnez **Options VM**.

4 Cliquez sur **Avancées**, puis cliquez sur **Modifier la configuration**.

5 Définissez les paramètres suivants sur TRUE en les ajoutant ou en les modifiant.

   - `isolation.tools.unity.push.update.disable`
   - `isolation.tools.ghi.launchmenu.change`
   - `isolation.tools.memSchedFakeSampleStats.disable`
   - `isolation.tools.getCreds.disable`
   - `isolation.tools.ghi.autologon.disable`
   - `isolation.bios.bbs.disable`
   - `isolation.tools.hgfsServerSet.disable`

6 Cliquez sur **OK**.

Désactiver les transferts de fichiers HGFS

Certaines opérations telles que les mises à niveau de VMware Tools automatisées utilisent le composant HGFS (Host Guest File System) de l'hyperviseur. Dans les environnement hautement sécurisés, vous pouvez désactiver ce composant pour minimiser le risque d'utilisation du système HGFS par un pirate pour transférer des fichiers dans le système d'exploitation invité.

Procédure

1 Connectez-vous à un système vCenter Server à l'aide de vSphere Web Client et localisez la machine virtuelle.

   a Dans le navigateur, sélectionnez **VM et modèles**.

   b Localisez la machine virtuelle dans la hiérarchie.

2 Cliquez avec le bouton droit sur la machine virtuelle et cliquez sur**Modifier les paramètres**.

3 Sélectionnez **Options VM**.

4 Cliquez sur **Avancées**, puis cliquez sur **Modifier la configuration**.

5 Vérifiez que le paramètre `isolation.tools.hgfsServerSet.disable` est défini sur TRUE.

Lorsque vous apportez cette modification, le processus VMX ne répond plus aux commandes du processus tools. Les API qui utilisent HGFS pour transférer des fichiers vers et depuis le système d'exploitation invité, telles que certaines commandes VIX ou l'utilitaire `auto-upgrade` de VMware Tools, ne fonctionnent plus.

Désactiver les opérations Copier et Coller entre le système d'exploitation client et la console distante

Les opérations Copier et Coller entre le système d'exploitation hôte et la console distante sont désactivées par défaut. Pour un environnement sécurisé, conservez ce paramétrage par défaut. Si vous avez besoin d'effectuer des opérations Copier et Coller, vous devez les activer en utilisantvSphere Web Client.

Ces options sont réglées sur la valeur recommandée par défaut. Toutefois, vous devez les régler sur vrai explicitement si vous souhaitez activer des outils d'audit pour vérifier que le réglage est correct.

Prérequis

Désactivez la machine virtuelle.

Procédure

1 Ouvrez une session sur un système vCenter Server au moyen de vSphere Web Client.

2 Cliquez avec le bouton droit sur la machine virtuelle et cliquez sur**Modifier les paramètres**.

3 Cliquez sur **Options VM**, puis cliquez sur **Modifier la configuration**.

4 Assurez-vous que les valeurs suivantes sont dans les colonnes de nom et de valeur, ou cliquez sur **Ajouter ligne** pour les ajouter.

Nom	Valeur recommandée
isolation.tools.copy.disable	vrai
isolation.tools.paste.disable	vrai
isolation.tools.setGUIOptions.enable	false

   Ces options écrasent les valeurs entrées dans Panneau de configuration de VMware Tools, sur le système d'exploitation invité.

5 Cliquez sur **OK**.

6 (Facultatif) Si vous avez modifié les paramètres de configuration, redémarrez la machine virtuelle.

Limitation de l'exposition des données sensibles copiées dans le presse-papiers

Par défaut, les opérations Copier et Coller sont désactivées pour les hôtes, afin d'éviter d'exposer les données sensibles copiées dans le presse-papiers.

Lorsque les opérations Copier et Coller sont activées sur une machine virtuelle utilisant VMware Tools, vous pouvez copier et coller des données entre le système d'exploitation invité et la console distante. Dès que la fenêtre de la console s'affiche, les utilisateurs et les processus ne disposant pas de privilèges d'accès et utilisant la machine virtuelle peuvent accéder au presse-papiers de sa console. Si un utilisateur copie des informations sensibles dans le presse-papiers avant d'utiliser la console, il expose (involontairement) des données sensibles au niveau de la machine virtuelle. Pour éviter ce problème, les opérations Copier et Coller sont par défaut désactivées sur le système d'exploitation invité.

En cas de besoin, vous pouvez activer ces opérations pour les machines virtuelles.

Empêcher des utilisateurs d'exécuter des commandes dans une machine virtuelle

Par défaut, un utilisateur avec le rôle Administrateur de vCenter Server peut interagir avec les fichiers et les applications au sein du système d'exploitation invité d'une machine virtuelle. Afin de réduire les risques d'atteinte à la confidentialité, la disponibilité et l'intégrité de l'invité, créez un rôle d'accès non-invité, dépourvu du privilège **Opérations client**. Attribuez ce rôle aux administrateurs qui n'ont pas besoin d'avoir accès aux fichiers de la machine virtuelle.

Pour garantir la sécurité, appliquez les mêmes restrictions pour l'accès au centre de données virtuel que pour l'accès au centre de données physique. Appliquez un rôle personnalisé qui désactive l'accès invité aux utilisateurs qui ont besoin de privilèges d'administrateur mais qui ne sont pas autorisés à interagir avec les fichiers et les applications du système d'exploitation invité.

Prenons, par exemple, une configuration composée d'une machine virtuelle placée dans une infrastructure contenant des informations sensibles.

Si des tâches telles que la migration avec vMotion nécessitent que les administrateurs de centre de données puissent accéder à la machine virtuelle, désactivez certaines opérations sur le système d'exploitation invité afin que ces administrateurs ne puissent pas accéder aux informations sensibles.

Prérequis

Vérifiez que vous avez les privilèges **Administrateur** sur le système vCenter Server sur lequel vous créez le rôle.

Procédure

1 Connectez-vous à vSphere Web Client en tant qu'utilisateur possédant des privilèges **Administrateur** sur le système vCenter Server sur lequel vous créez le rôle.

2 Cliquez sur **Administration** et sélectionnez **Rôles**.

3 Cliquez sur l'icône **Créer une action de rôle** et tapez le nom que vous souhaitez attribuer au rôle.

Par exemple, entrez **`Accès non-invité administrateur`**.

4 Sélectionnez **Tous les privilèges**.

5 Désélectionnez **Tous les privilèges.Machine virtuelle.Systèmes invités** pour supprimer l'ensemble des privilèges pour les opérations sur les systèmes invités.

6 Cliquez sur **OK**.

Suivant

Sélectionnez le système vCenter Server ou l'hôte et attribuez une autorisation qui couple l'utilisateur ou le groupe requérant les nouveaux privilèges avec le rôle que vous venez de créer. Supprimez ces utilisateurs du rôle Administrateur.

Empêcher les utilisateurs ou les processus de machines virtuelles de déconnecter les périphériques

Les utilisateurs et les processus sans privilèges racine ou d'administrateur au sein des machines virtuelles ont la possibilité de connecter ou déconnecter des périphériques, comme les adaptateurs réseau et les lecteurs de CD-ROM, et peuvent modifier leurs paramètres. Afin de renforcer la sécurité des machines virtuelles, supprimez ces périphériques. Si vous ne souhaitez qu'un périphérique soit supprimé, vous pouvez modifier les paramètres du système d'exploitation invité pour empêcher les utilisateurs ou les processus de modifier son état.

Prérequis

Désactivez la machine virtuelle.

Procédure

1 Connectez-vous à un système vCenter Server à l'aide de vSphere Web Client et localisez la machine virtuelle.

   a Dans le navigateur, sélectionnez **VM et modèles**.

   b Localisez la machine virtuelle dans la hiérarchie.

2 Cliquez avec le bouton droit sur la machine virtuelle et cliquez sur**Modifier les paramètres**.

3 Sélectionnez **Options VM**.

4 Cliquez sur **Avancées**, puis cliquez sur **Modifier la configuration**.

5 Vérifiez que les valeurs suivantes sont dans les colonnes de nom et de valeur, ou cliquez sur **Ajouter ligne** pour les ajouter.

Nom	Valeur
isolation.device.connectable.disable	vrai
isolation.device.edit.disable	vrai

   Ces options écrasent les valeurs entrées dans Panneau de configuration de VMware Tools, sur le système d'exploitation invité.

6 Cliquez sur **OK** pour fermer la boîte de dialogue Paramètres de configuration, puis cliquez de nouveau sur **OK**.

Empêcher les processus du système d'exploitation invité d'envoyer des messages de configuration à l'hôte

Pour vous assurer que le système d'exploitation invité ne modifie par les paramètres de configuration, vous pouvez empêcher ces processus d'écrire des paires nom-valeur dans le fichier de configuration.

Prérequis

Désactivez la machine virtuelle.

Procédure

1 Connectez-vous à un système vCenter Server à l'aide de vSphere Web Client et localisez la machine virtuelle.

   a Dans le navigateur, sélectionnez **VM et modèles**.

   b Localisez la machine virtuelle dans la hiérarchie.

2 Cliquez avec le bouton droit sur la machine virtuelle et cliquez sur**Modifier les paramètres**.

3 Sélectionnez **Options VM**.

4 Cliquez sur **Avancées**, puis cliquez sur **Modifier la configuration**.

5 Cliquez sur **Ajouter ligne** et tapez les valeurs suivantes dans les colonnes de nom et de valeur.

Colonne	Valeur
Nom	`isolation.tools.setinfo.disable`
Valeur	`vrai`

6 Cliquez sur **OK** pour fermer la boîte de dialogue Paramètres de configuration, puis cliquez de nouveau sur **OK**.

Éviter d'utiliser des disques indépendants non persistants

Lorsque vous utilisez des disques indépendants non permanents, des pirates peuvent supprimer toute évidence que la machine a été compromise en arrêtant ou en redémarrant le système. Sans un enregistrement permanent des activités sur une machine virtuelle, une attaque risque de ne pas être décelée par les administrateurs. Il convient donc d'éviter d'utiliser des disques indépendants non permanents.

Procédure

- Assurez-vous que l'activité de la machine virtuelle est consignée à distance sur un serveur séparé, par exemple un serveur syslog ou un collecteur d'événements Windows équivalent.

  Si la journalisation à distance des événements n'est pas configurée pour l'invité, scsiX:Y.mode doit prendre l'une des valeurs suivantes :

  - Pas présent
  - Non défini sur indépendant non permanent

Lorsque le mode non permanent n'est pas activé, vous ne pouvez pas remettre une machine virtuelle à un état connu lors du redémarrage du système.

Chiffrement des machines virtuelles 6

À partir de vSphere 6.5, vous pouvez bénéficier du chiffrement des machines virtuelles. Le chiffrement protège non seulement votre machine virtuelle mais également les disques de machine virtuelle et autres fichiers. Vous configurez une connexion approuvée entre vCenter Server et un serveur de gestion des clés (KMS). vCenter Server peut ensuite récupérer des clés du serveur de gestion des clés si nécessaire.

Vous gérez les divers aspects du chiffrement des machines virtuelles de façons différentes.

- Gérez la configuration de la connexion approuvée à l'aide du serveur de gestion des clés et effectuez les principaux workflows du chiffrement à partir de vSphere Web Client.
- Gérez l'automatisation de certaines fonctionnalités avancées à partir de vSphere Web Services SDK. Reportez-vous aux sections *Guide de programmation de vSphere Web Services SDK* et *Référence de VMware vSphere API*.
- Utilisez l'outil de ligne de commande `crypto-util`directement sur l'hôte ESXi pour certains cas spéciaux, par exemple, pour déchiffrer les vidages de mémoire dans un bundle `vm-support`.

Présentation du chiffrement des machines virtuelles vSphere (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vsphere_virtual_machine_encryption_overview)

Ce chapitre aborde les rubriques suivantes :

Méthodologie utilisée par le chiffrement de machine virtuelle vSphere pour protéger votre environnement

Le chiffrement de machine virtuelle vSphere vous permet de créer des machines virtuelles chiffrées et de chiffrer des machines virtuelles existantes. Étant donné que tous les fichiers de machine virtuelle contenant des informations sensibles sont chiffrés, la machine virtuelle est protégée. Seuls les administrateurs disposant de privilèges de chiffrement peuvent effectuer des tâches de chiffrement et de déchiffrement.

Clés utilisées

Deux types de clés sont utilisés pour le chiffrement.

- L'hôte ESXi génère et utilise des clés internes pour chiffrer des machines virtuelles et des disques. Ces clés sont utilisées en tant que chiffrement de base de données (DEK). Ce sont des clés XTS AES 256 bits.
- vCenter Server demande les clés au certificat KMS. Ces clés sont utilisées en tant que clés de chiffrement de clés (KEK) et sont des clés AES 256 bits. vCenter Server stocke uniquement l'identifiant de chaque KEK et non la clé elle-même.
- ESXi utilise la clé KEK pour chiffrer les clés internes et stocke la clé interne chiffrée sur le disque. ESXi ne stocke pas la clé KEK sur le disque. Lorsqu'un hôte redémarre, vCenter Server demande la clé KEK avec l'ID correspondant au KMS et la met à la disposition du produit ESXi. ESXi peut alors déchiffrer les clés internes si nécessaire.

Éléments chiffrés

Le chiffrement de machine virtuelle vSphere prend en charge le chiffrement des fichiers de machine virtuelle, les fichiers de disque virtuel et les fichiers de vidage de mémoire.

fichiers de machine virtuelle

La plupart des fichiers de machine virtuelle, notamment les données invitées qui ne sont pas stockées dans le fichier VMDK, sont chiffrés. Cet ensemble de fichiers inclut les fichiers NVRAM, VSWP et VMSN, sans se limiter à ceux-ci. La clé que vCenter Server récupère auprès de KMS déverrouille un bundle chiffré dans le fichier VMX qui contient des clés internes et d'autres secrets.

Si vous utilisez vSphere Web Client pour créer une machine virtuelle chiffrée, tous les disques virtuels sont chiffrés par défaut. Pour d'autres tâches de chiffrement, comme le chiffrement d'une machine virtuelle existante, vous pouvez chiffrer et déchiffrer des disques virtuels distincts des fichiers de machine virtuelle.

Remarque Vous ne pouvez pas associer un disque virtuel chiffré à une machine virtuelle qui n'est pas chiffrée.

fichiers de disque virtuel

Les données se trouvant dans un fichier de disque virtuel (VMDK) chiffré ne sont jamais écrites en texte clair dans le stockage ou le disque physique, et elles ne sont jamais transmises sur le réseau en texte clair. Le fichier descripteur VMDK est principalement en texte clair, mais il contient un ID de clé pour la clé KEK et la clé interne (DEK) dans le bundle chiffré.

Vous pouvez utiliser vSphere API pour effectuer une opération de rechiffrement de premier niveau avec une nouvelle clé KEK ou une opération de rechiffrement approfondi avec une nouvelle clé interne.

vidages de mémoire

Les vidages de mémoire sur un hôte ESXi pour lequel le mode de chiffrement est activé sont toujours chiffrés. Reportez-vous à « Chiffrement de machines virtuelles vSphere et vidages mémoire », page 159.

Remarque Les vidages de mémoire sur le système vCenter Server ne sont pas chiffrés. Veillez à protéger l'accès au système vCenter Server.

Remarque Pour plus d'informations sur certaines des limites relatives aux dispositifs et aux fonctionnalités avec lesquels le chiffrement de machine virtuelle vSphere peut interagir, reportez-vous à la section « Interopérabilité du chiffrement des machines virtuelles », page 145.

Éléments non chiffrés

Certains des fichiers associés à une machine virtuelle ne sont pas chiffrés ou sont partiellement chiffrés.

fichiers de journalisation

Les fichiers de journalisation ne sont pas chiffrés, car ils ne contiennent pas de données sensibles.

fichiers de configuration de machine virtuelle

La plupart des informations de configuration de machine virtuelle stockées dans les fichiers VMX et VMSD ne sont pas chiffrées.

fichier descripteur du disque virtuel

Pour permettre la gestion de disque sans clé, la plus grande partie du fichier descripteur du disque virtuel n'est pas chiffrée.

Personnes habilitées à effectuer des opérations cryptographiques

Seuls les utilisateurs auxquels des privilèges d'**opérations cryptographiques** ont été attribués peuvent effectuer des opérations de chiffrement. L'ensemble de privilèges est détaillé. Reportez-vous à « Privilèges d'opérations de chiffrement », page 198. Le rôle d'administrateur système par défaut possède tous les privilèges d'**opérations cryptographiques**. Un nouveau rôle, celui d'administrateur sans cryptographie, prend en charge tous les privilèges d'administrateur à l'exception des privilèges d'**opérations cryptographiques**.

Vous pouvez créer des rôles personnalisés supplémentaires, par exemple pour autoriser un groupe d'utilisateurs à chiffrer des machines virtuelles tout en les empêchant de déchiffrer des machines virtuelles.

Méthodologie pour effectuer des opérations cryptographiques

vSphere Web Client prend en charge de nombreuses opérations cryptographiques. Pour d'autres tâches, vous pouvez utiliser vSphere API.

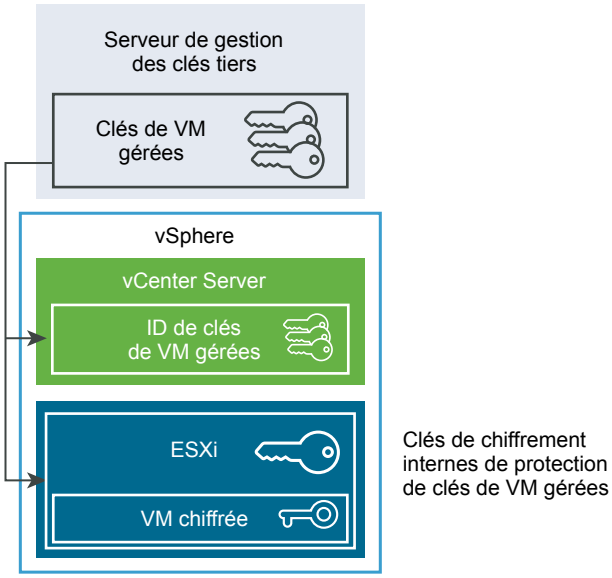
Tableau 6-1. Interfaces pour l'exécution d'opérations cryptographiques

Interface	Opérations	Informations
vSphere Web Client	Créer une machine virtuelle chiffrée Chiffrer et déchiffrer des machines virtuelles	Ce livre.
vSphere Web Services SDK	Créer une machine virtuelle chiffrée Chiffrer et déchiffrer des machines virtuelles Effectuez un rechiffrement approfondi d'une machine virtuelle (utilisez une clé DEK différente). Effectuez un rechiffrement de premier niveau d'une machine virtuelle (utilisez une clé KEK différente).	*Guide de programmation de vSphere Web Services SDK* *Référence de VMware vSphere API*
`crypto-util`	Déchiffrez des vidages de mémoire chiffrés, déterminez si des fichiers sont chiffrés et effectuez d'autres tâches de gestion directement sur l'hôte ESXi.	Aide relative à la ligne de commande. « Chiffrement de machines virtuelles vSphere et vidages mémoire », page 159

Composants du chiffrement des machines virtuelles vSphere

Un serveur de gestion des clés externe, le système vCenter Server et vos hôtes ESXi sont les principaux composants de la solution Chiffrement des machines virtuelles vSphere.

Figure 6-1. Architecture de chiffrement virtuel de vSphere



Serveur de gestion des clés

vCenter Server demande des clés auprès d'un serveur de gestion des clés externe. Ce dernier génère et stocke les clés, et les transmet à vCenter Server pour distribution.

Vous pouvez utiliser vSphere Web Client ou vSphere API pour ajouter un cluster d'instances KMS au système vCenter Server. Si vous utilisez plusieurs instances KMS dans un cluster, toutes les instances doivent provenir du même fournisseur et doivent répliquer des clés.

Si votre environnement utilise différents fournisseurs KMS dans différents environnements, vous pouvez ajouter un cluster KMS pour chaque serveur de gestion des clés et spécifier un cluster KMS par défaut. Le premier cluster ajouté devient le cluster par défaut. Vous pouvez spécifier la valeur par défaut ultérieurement.

En tant que client KMIP, vCenter Server utilise le protocole KMIP (Key Management Interoperability Protocol) pour faciliter l'utilisation du serveur de gestion des clés de votre choix.

vCenter Server

Seul vCenter Server détient les informations d'identification pour établir la connexion au serveur de gestion des clés. Vos hôtes ESXi ne possèdent pas ces informations d'identification. vCenter Server obtient des clés du serveur de gestion des clés et les transmet aux hôtes ESXi. vCenter Server ne stocke pas les clés KMS mais conserve une liste des ID de clé.

vCenter Server vérifie les privilèges des utilisateurs qui effectuent des opérations de chiffrement. Vous pouvez utiliser vSphere Web Client pour attribuer des privilèges pour les opérations de chiffrement ou pour attribuer le rôle personnalisé **Aucun administrateur de chiffrement** aux groupes d'utilisateurs. Reportez-vous à « Conditions préalables et privilèges requis pour les tâches de chiffrement », page 140.

vCenter Server ajoute des événements cryptographiques à la liste des événements que vous pouvez afficher et exporter à partir de la console des événements de vSphere Web Client. Chaque événement inclut l'utilisateur, l'heure, l'ID de clé et l'opération de chiffrement.

Les clés provenant du serveur de gestion des clés sont utilisées comme clés de chiffrement de clés (KEK).

Hôtes ESXi

Les hôtes ESXi sont responsables de plusieurs aspects du workflow de chiffrement.

- vCenter Server transmet les clés à un hôte ESXi lorsque ce dernier en a besoin. Le mode de chiffrement doit être activé pour l'hôte. Le rôle de l'utilisateur actuel doit inclure des privilèges d'opération de chiffrement. Reportez-vous aux sections « Conditions préalables et privilèges requis pour les tâches de chiffrement », page 140 et « Privilèges d'opérations de chiffrement », page 198.
- Garantir que les données de l'invité pour les machines virtuelles chiffrées sont chiffrées lorsqu'elles sont stockées sur disque.
- Garantir que les données de l'invité pour les machines virtuelles chiffrées ne sont pas envoyées sur le réseau sans être chiffrées.

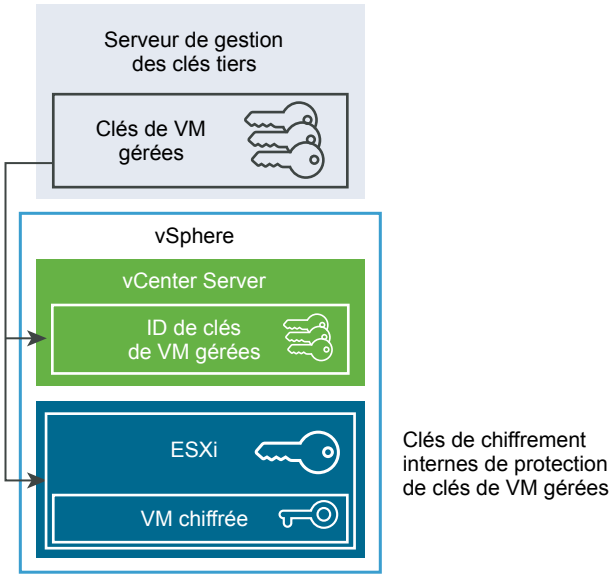
Les clés générées par l'hôte ESXi sont appelées clés internes dans ce document. Ces clés jouent généralement le rôle de clés de chiffrement de données (DEK).

Flux de chiffrement

Une fois vCenter Server connecté au KMS, les utilisateurs disposant des privilèges requis peuvent créer des machines virtuelles et des disques chiffrés. Ces utilisateurs peuvent également exécuter d'autres tâches de chiffrement, telles que le chiffrement de machines virtuelles existantes et le déchiffrement de machines virtuelles chiffrées.

Le flux inclut le KMS, vCenter Server et l'hôte ESXi.

Figure 6-2. Architecture de chiffrement virtuel de vSphere



Pendant le processus de chiffrement, différents composants vSphere interagissent de la façon suivante.

1 Lorsque l'utilisateur exécute une tâche de chiffrement, par exemple pour créer une machine virtuelle, vCenter Server demande une nouvelle clé au KMS par défaut. Cette clé sera utilisée en tant que certificat KEK (Key Exchange Key).

2 vCenter Server stocke l'identifiant de clé et transmet la clé à l'hôte ESXi. Si l'hôte ESXi fait partie d'un cluster, vCenter Server envoie le certificat KEK à chacun des hôtes du cluster.

   La clé, quant à elle, n'est pas stockée sur le système vCenter Server. Seul l'identifiant de clé est connu.

3 L'hôte ESXi génère des clés internes (DEK) pour la machine virtuelle et ses disques. Les clés internes sont conservées uniquement en mémoire et l'hôte utilise les certificats KEK pour chiffrer les clés internes.

   Les clés internes non chiffrées ne sont jamais stockées sur disque. Seules les données chiffrées sont stockées. Dans la mesure où les certificats KEK proviennent du KMS, l'hôte continue d'utiliser les mêmes KEK.

4 L'hôte ESXi chiffre la machine virtuelle avec la clé interne chiffrée.

   Tous les hôtes qui ont le certificat KEK et peuvent accéder au fichier de clé chiffrée peuvent exécuter des opérations sur la machine virtuelle chiffrée ou le disque.

Si vous souhaitez ensuite déchiffrer une machine virtuelle, vous pouvez modifier sa stratégie de stockage. Vous pouvez modifier la stratégie de stockage de la machine virtuelle et de l'ensemble des disques. Si vous souhaitez déchiffrer des composants individuels, déchiffrez les disques sélectionnés en premier, puis déchiffrez la machine virtuelle en modifiant la stratégie de stockage d'Accueil VM. Les deux clés sont nécessaires pour le déchiffrement de chaque composant.

Chiffrement de machines virtuelles et de disques (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_encrypting_vms_and_disks)

Chiffrement des disques virtuels

Lorsque vous créez une machine virtuelle chiffrée à partir de vSphere Web Client, tous les disques virtuels sont chiffrés. Vous pouvez, par la suite, ajouter des disques et définir leur stratégies de chiffrement. Vous ne pouvez pas ajouter un disque chiffré à une machine virtuelle qui n'est pas chiffrée, et vous ne pouvez pas chiffrer un disque si la machine virtuelle n'est pas chiffrée.

Le chiffrement d'une machine virtuelle et de ses disques est contrôlé à l'aide de stratégies de stockage. La stratégie de stockage d'Accueil VM gouverne la machine virtuelle elle-même, et chaque disque virtuel a une stratégie de stockage associée.

- Définir la stratégie de stockage d'Accueil VM sur une stratégie de chiffrement chiffre uniquement la machine virtuelle en elle-même.
- Définir la stratégie de stockage d'Accueil VM et de tous les disques sur une stratégie de chiffrement chiffre l'ensemble des composants.

Examinez les cas d'utilisation suivants.

Tableau 6-2. Cas d'utilisation de chiffrement des disques virtuels

Cas d'utilisation	Détails
Créer une machine virtuelle chiffrée	Si vous ajoutez des disques pendant que vous créez une machine virtuelle chiffrée, les disques sont chiffrés par défaut. Vous pouvez modifier la stratégie de manière à ne pas chiffrer un ou plusieurs disques. Après la création de la machine virtuelle, vous pouvez modifier explicitement la stratégie de stockage de chaque disque. Reportez-vous à « Modifier la stratégie de chiffrement des disques virtuels », page 158.
Chiffrez une machine virtuelle.	Pour chiffrer une machine virtuelle existante, vous modifiez sa stratégie de stockage. Vous pouvez modifier la stratégie de stockage pour la machine virtuelle et pour tous les disques virtuels. Pour chiffrer uniquement la machine virtuelle, vous pouvez spécifier une stratégie de chiffrement d'Accueil VM et sélectionnez une stratégie de stockage différente, comme Valeur par défaut de la banque de données, pour chaque disque virtuel.
Ajouter un disque non chiffré existant à une machine virtuelle chiffrée (stratégie de stockage de chiffrement)	Échoue avec une erreur. Vous devez ajouter le disque avec la stratégie de stockage par défaut, mais vous pourrez modifier la stratégie de stockage ultérieurement.
Ajoutez un disque non chiffré existant à une machine virtuelle chiffrée avec une stratégie de stockage qui n'inclut pas le chiffrement, par exemple Valeur par défaut de la banque de données.	Le disque utilise la stratégie de stockage par défaut. Vous pouvez modifier explicitement la stratégie de stockage après avoir ajouté le disque si vous souhaitez un disque chiffré.
Ajoutez un disque chiffré à une machine virtuelle chiffrée. La stratégie de stockage d'Accueil VM est Chiffrement.	Lorsque vous ajoutez le disque, il reste chiffré. vSphere Web Client affiche la taille et d'autres attributs, y compris l'état de chiffrement, mais il est possible qu'il n'affiche pas la stratégie de stockage correcte. Pour des raisons de cohérence, modifiez la stratégie de stockage.
Ajouter un disque chiffré existant à une machine virtuelle non chiffrée	Ce cas d'utilisation n'est pas pris en charge.

Conditions préalables et privilèges requis pour les tâches de chiffrement

Les tâches de chiffrement sont possibles uniquement dans les environnements qui incluent vCenter Server. De plus, le mode de chiffrement doit être activé sur l'hôte ESXi pour la plupart des tâches de chiffrement. L'utilisateur qui exécute la tâche doit disposer des privilèges appropriés. Un ensemble de privilèges **Opérations de chiffrement** permet d'effectuer un contrôle plus précis. Si des tâches de chiffrement de machines virtuelles nécessitent de modifier le mode de chiffrement de l'hôte, des privilèges supplémentaires sont requis.

Privilèges de chiffrement et rôles

Par défaut, l'utilisateur ayant le rôle d'vCenter Serveradministrateur détient tous les privilèges. Le rôle **Aucun administrateur de chiffrement** ne dispose pas des privilèges suivant qui sont requis pour les opérations de chiffrement.

- Ajoutez des privilèges **Opérations de chiffrement**.
- **Global.Diagnostics**
- **Hôte.Inventaire.Ajouter hôte au cluster**
- **Hôte.Inventaire.Ajouter un hôte autonome**
- **Hôte.Opérations locales.Gérer des groupes d'utilisateurs**

Vous pouvez attribuer le rôle **Aucun administrateur de chiffrement** à des vCenter Server administrateurs qui n'ont pas besoin de privilèges **Opérations de chiffrement**.

Pour limiter davantage ce que les utilisateurs sont autorisés à faire, vous pouvez cloner le rôle **Aucun administrateur de chiffrement** et créer un rôle personnalisé avec certains privilèges **Opérations de chiffrement** uniquement. Par exemple, vous pouvez créer un rôle qui permet aux utilisateurs de chiffrer, mais pas de déchiffrer des machines virtuelles, ou qui attribue des privilèges pour des opérations de gestion. Reportez-vous à « Utilisation des rôles pour assigner des privilèges », page 32.

Mode de chiffrement de l'hôte

Vous ne pouvez chiffrer de machines virtuelles que si le mode de chiffrement de l'hôte est activé pour l'hôte ESXi. Le mode de chiffrement de l'hôte est automatiquement activé, mais il peut être activé explicitement. Vous pouvez vérifier et définir explicitement le mode de chiffrement de l'hôte actuel depuis vSphere Web Client ou à l'aide de vSphere API.

Voir « Activer explicitement le mode de chiffrement de l'hôte », page 154 pour des instructions.

Une fois le mode de chiffrement de l'hôte activé, celui-ci ne peut pas être désactivé facilement. Reportez-vous à « Désactiver le mode de chiffrement de l'hôte », page 154.

Des modifications automatiques se produisent lorsque des opérations de chiffrement tentent d'activer le mode de chiffrement de l'hôte. Supposez par exemple que vous ajoutez une machine virtuelle chiffrée à un hôte autonome et que le mode de chiffrement de l'hôte n'est pas activé. Si vous disposez des privilèges requis sur l'hôte, le mode de chiffrement devient automatiquement activé.

Supposez qu'un cluster dispose de trois hôtes ESXi, A, B et C. Vous ajoutez une machine virtuelle chiffrée à l'hôte A. L'effet produit dépend de plusieurs facteurs.

- Si le chiffrement pour les hôtes A, B et C est déjà activé, vous avez uniquement besoin des privilèges **Opérations de chiffrement.Chiffrer nouvel élément** pour pouvoir créer la machine virtuelle.

- Si les hôtes A et B sont activés pour le chiffrement et que C n'est pas activé, le système procède de la manière suivante.
  - Si vous disposez des privilèges **Opérations de chiffrement.Chiffrer nouvel élément** et **Opérations de chiffrement.Enregistrer l'hôte** sur chacun des hôtes, le processus de création de machine virtuelle permet alors le chiffrement sur l'hôte C. Le processus de chiffrement active le mode de chiffrement de l'hôte sur l'hôte C, et transmet la clé à chaque hôte du cluster.

    Dans ce cas, vous pouvez également activer explicitement le chiffrement de l'hôte sur l'hôte C.
  - Si vous disposez uniquement des privilèges **Opérations de chiffrement.Chiffrer nouvel élément** sur la machine virtuelle ou le dossier de la machine virtuelle, la création de la machine virtuelle réussit et la clé devient disponible sur l'hôte A et l'hôte B. L'hôte C est toujours désactivé pour le chiffrement et ne dispose pas de la clé de la machine virtuelle.
- Si aucun des hôtes n'est activé pour le chiffrement et que vous disposez des privilèges **Opérations de chiffrement.Enregistrer l'hôte** sur l'hôte A, le processus de création de machine virtuelle active le chiffrement de l'hôte sur cet hôte. Sinon, une erreur se produit.

Conditions requises en matière d'espace disque

Lorsque vous chiffrez une machine virtuelle existante, vous avez besoin d'au moins deux fois l'espace en cours d'utilisation par la machine virtuelle.

vSphere vMotion chiffré

À partir de vSphere 6.5, vSphere vMotion applique systématiquement le chiffrement lors de la migration de machines virtuelles chiffrées. Pour les machines virtuelles qui ne sont pas chiffrées, vous pouvez sélectionner l'une des options chiffrées de vSphere vMotion.

La version chiffrée de vSphere vMotion garantit la confidentialité, l'intégrité et l'authenticité des données qui sont transférées avec vSphere vMotion. La version chiffrée de vSphere vMotion prend en charge toutes les variantes de vSphere vMotion pour les machines virtuelles non chiffrées, ce qui inclut la migration sur les différents systèmes vCenter Server. La migration sur les systèmes vCenter Server n'est pas prise en charge pour les machines virtuelles chiffrées.

Concernant les disques chiffrés, les données sont transmises chiffrées. Pour les disques qui ne sont pas chiffrés, le chiffrement par Storage vMotion n'est pas pris en charge.

Lorsque les machines virtuelles sont chiffrées, la migration avec vSphere vMotion utilise systématiquement la version chiffrée de vSphere vMotion. Vous ne pouvez pas désactiver le chiffrement de vSphere vMotion pour les machines virtuelles chiffrées.

Concernant les machines virtuelles qui ne sont pas chiffrées, vous pouvez définir vSphere vMotion à l'un des états suivants. La valeur par défaut est Opportuniste.

Désactivé	N'utilisez pas vSphere vMotion chiffré.
Opportuniste	Utilisez vSphere vMotion chiffré si les hôtes source et de destination le prennent en charge. Seules les versions 6.5 et ultérieures de ESXi utilisent vSphere vMotion chiffré.
Requis	Autorisez uniquement vSphere vMotion chiffré. Si l'hôte source ou de destination ne prend pas en charge vSphere vMotion chiffré, la migration avec vSphere vMotion est interdite.

Lorsque vous chiffrez une machine virtuelle, cette dernière conserve une trace du paramètre vSphere vMotion actuellement chiffré. Si vous désactivez par la suite le chiffrement de la machine virtuelle, le paramètre vMotion chiffré demeure au niveau Requis jusqu'à ce que vous le changiez de façon explicite. Vous pouvez modifier les paramètres avec l'option **Modifier les paramètres**.

Reportez-vous à la documentation de *Gestion de vCenter Server et des hôtes* pour plus d'informations sur l'activation et la désactivation de vSphere vMotion pour les machines virtuelles qui ne sont pas chiffrées.

Meilleures pratiques de chiffrement, mises en garde et interopérabilité

Les meilleures pratiques et mises en garde relatives au chiffrement des machines physiques s'appliquent également aux machines virtuelles. L'architecture de chiffrement de machine virtuelle donne lieu à des recommandations supplémentaires. Tenez compte des limitations d'interopérabilité pendant la phase de planification de la stratégie de chiffrement des machines virtuelles.

Meilleures pratiques de chiffrement des machines virtuelles

Suivez les meilleures pratiques de chiffrement des machines virtuelles pour éviter les problèmes ultérieurement, par exemple, lorsque vous générez un bundle `vm-support`.

Meilleures pratiques générales

Suivez les meilleures pratiques générales suivantes pour éviter les problèmes.

- Ne chiffrez pas une machine virtuelle vCenter Server Appliance.
- Si votre hôte ESXi plante, récupérez le bundle de support dès que possible. La clé de l'hôte doit être disponible si vous voulez générer un bundle de support utilisant un mot de passe ou si vous voulez déchiffrer le vidage de mémoire. Si l'hôte est redémarré, il est possible que la clé de l'hôte change et que vous ne puissiez plus générer un bundle de support avec un mot de passe ou déchiffrer des vidages de mémoire dans le bundle de support à l'aide de la clé de l'hôte.
- Gérez les noms de cluster du serveur de gestion des clés avec précaution. Si le nom de cluster du serveur de gestion des clés change pour un serveur de gestion des clés déjà utilisé, les machines virtuelles chiffrées à l'aide des clés de ce serveur prennent un état non valide pendant la mise sous tension ou l'enregistrement. Dans ce cas, supprimez le serveur de gestion des clés à partir de vCenter Server et ajoutez-le avec le nom de cluster que vous avez utilisé au départ.
- Ne modifiez pas les fichiers VMX et les fichiers descripteurs VMDK. Ces fichiers contiennent le bundle de chiffrement. Il est possible que vos modifications rendent la machine virtuelle irrécupérable et que le problème de récupération ne puisse pas être résolu.
- Le processus de chiffrement chiffre les données sur l'hôte avant qu'elles soient écrites dans le stockage. Les fonctionnalités de stockage centralisé comme la déduplication et la compression peuvent ne pas être performantes pour les machines virtuelles chiffrées. Lorsque vous utilisez le chiffrement des machines virtuelles vSphere, envisagez d'effectuer des compromis de stockage.
- Le chiffrement nécessite une utilisation importante du CPU. AES-NI améliore de manière significative les performances du chiffrement. Activez AES-NI dans votre BIOS.

Meilleures pratiques pour les vidages de mémoire chiffrés

Suivez ces meilleures pratiques pour éviter les problèmes lorsque vous devez examiner un vidage de mémoire dans le cadre du diagnostic d'un incident.

- Établissez une stratégie concernant les vidages de mémoire. Les vidages de mémoire sont chiffrés, car ils peuvent contenir des informations sensibles telles que des clés. Si vous déchiffrez un vidage de mémoire, prenez en compte ses informations sensibles. Les vidages de mémoire ESXi peuvent contenir des clés de l'hôte ESXi des machines virtuelles qui s'y trouvent. Envisagez de modifier la cl de l'hôte et de rechiffrer les machines virtuelles chiffrées après avoir déchiffré un vidage de mémoire. Vous pouvez effectuer ces deux tâches à l'aide de vSphere API.

  Reportez-vous à « Chiffrement de machines virtuelles vSphere et vidages mémoire », page 159 pour plus de détails.

- Utilisez toujours un mot de passe lorsque vous collectez un bundle `vm-support`. Vous pouvez spécifier le mot de passe lorsque vous générez le bundle de support à partir de vSphere Web Client ou à l'aide de la commande `vm-support`.

  Le mot de passe rechiffre les vidages de mémoire utilisant des clés internes de façon à utiliser les clés reposant sur le mot de passe. Vous pouvez utiliser ultérieurement le mot de passe pour déchiffrer les vidages de mémoire chiffrés susceptibles d'être intégrés dans le bundle de support. Les vidages de mémoire ou les journaux non chiffrés ne sont pas concernés.

- Le mot de passe que vous spécifiez pendant la création du bundle `vm-support` n'est pas conservé dans les composants vSphere. Vous êtes responsable du suivi des mots de passe pour les bundles de support.
- Avant de modifier la clé de l'hôte, générez un bundle vm-support avec un mot de passe de façon à pouvoir accéder ultérieurement aux vidages de mémoire susceptibles d'être chiffrés avec l'ancienne clé de l'hôte.

Meilleures pratiques en matière de gestion du cycle de vie des clés

Mettez en œuvre les meilleures pratiques permettant de garantir la disponibilité du serveur de gestion des clés et de surveiller les clés sur ce serveur.

- Vous êtes responsable de la mise en place de stratégies garantissant la disponibilité du serveur de gestion des clés.

  Si le serveur de gestion des clés n'est pas disponible, il est impossible d'effectuer les opérations liées aux machines virtuelles nécessitant que vCenter Server demande la clé auprès du serveur de gestion des clés. Cela signifie que l'exécution des machines virtuelles se poursuit et que vous pouvez les mettre sous tension, mettre hors tension et reconfigurer. Toutefois, vous ne pouvez pas les déplacer vers un hôte qui ne dispose pas des informations concernant la clé.

  La plupart des solutions KMS incluent des fonctionnalités de haute disponibilité. Vous pouvez utiliser vSphere Web Client ou l'API pour spécifier le cluster de serveur de clés et les instances KMS associées.

- Vous êtes responsable du suivi des clés et de l'application de corrections sur les clés de machines virtuelles existantes ne sont pas à l'état Active.

  Le standard KMIP définit les états suivants pour les clés.

  - Pré-active
  - Active
  - Désactivée
  - Compromise
  - Détruite
  - Détruite compromise

  Le chiffrement des machines virtuelles vSphere utilise uniquement les clés à l'état Active pour la chiffrement. Si une clé est à l'état Pré-active, le chiffrement des machines virtuelles vSphere l'active. Si l'état de la clé est Désactivée, Compromise, Détruite ou Détruite compromise, cela signifie que vous ne pouvez pas chiffrer la machine virtuelle ou le disque virtuel présentant cet état.

  Pour les clés avec un autre état, les machines virtuelles correspondantes continuent de fonctionner. La réussite d'une opération de clonage ou de migration varie selon que la clé est déjà dans l'hôte ou non.

  - Si la clé est dans l'hôte de destination, l'opération réussit même si la clé n'est pas à l'état Active sur le serveur de gestion des clés.
  - Si les clés requises de la machine virtuelle et du disque virtuel ne sont pas dans l'hôte de destination, vCenter Server doit extraire les clés du serveur de gestion des clés. Si l'état de la clé est Désactivée, Compromise, Détruite ou Détruite compromise, vCenter Server affiche une erreur et l'opération échoue.

Une opération de clonage ou de migration réussit si la clé est déjà dans l'hôte. L'opération échoue si vCenter Server doit extraire les clés du serveur de gestion des clés.

Si une clé n'est pas à l'état Active, effectuez une opération de rechiffrement à l'aide de l'API. Reportez-vous au *Guide de programmation de vSphere Web Services SDK*.

Meilleures pratiques en matière de sauvegarde et de restauration

Configurez des stratégies pour les opérations de sauvegarde et de restauration.

- Toutes les architectures de sauvegarde ne sont pas prises en charge. Reportez-vous à « Interopérabilité du chiffrement des machines virtuelles », page 145.
- Configurez des stratégies pour les opérations de restauration. Étant donné que les sauvegardes sont toujours en texte clair, envisagez de chiffrer les machines virtuelles juste après la restauration. Vous pouvez spécifier que la machine virtuelle est chiffrée dans le cadre de l'opération de restauration. Si possible, chiffrez la machine virtuelle dans le cadre de l'opération de restauration pour éviter toute exposition des informations sensibles. Pour modifier la stratégie de chiffrement pour les disques associés à la machine virtuelle, modifiez la stratégie de stockage du disque.

Meilleures pratiques en matière de performances

- Les performances du chiffrement dépendent du CPU et de la vitesse du stockage.
- Le chiffrement de machines virtuelles existantes prend plus de temps que le chiffrement d'un machine virtuelle lors de sa création. Si possible, chiffrez une machine virtuelle au moment de la créer.

Meilleures pratiques en matière de stratégie de stockage

Ne modifiez pas l'exemple de stratégie de stockage du chiffrement des machines virtuelles. Au lieu de cela, clonez la stratégie et modifiez le clone.

Remarque Il n'existe aucun moyen automatisé de rétablir les paramètres d'origine de la stratégie de chiffrement des machines virtuelles.

Pour plus de détails sur la personnalisation des stratégies de stockage, reportez-vous à la documentation *Stockage vSphere*.

Mises en garde concernant le chiffrement des machines virtuelles

Prenez en compte les mises en garde concernant le chiffrement des machines virtuelles pour éviter l'apparition de problèmes.

Pour en savoir plus sur les dispositifs et les fonctionnalités qui ne peuvent pas être utilisés avec le chiffrement des machines virtuelles, reportez-vous à « Interopérabilité du chiffrement des machines virtuelles », page 145.

Limitations

Prenez en compte les mises en garde suivantes lorsque vous planifiez votre stratégie de chiffrement des machines virtuelles.

- Lorsque vous clonez une machine virtuelle chiffrée ou effectuez une opération de stockage vMotion, vous pouvez tenter de modifier le format de disque. Ces conversions ne sont pas toujours concluantes. Par exemple, si vous clonez une machine virtuelle et tentez de remplacer le format de disque en remplaçant le format statique mis à zéro en différé par le format dynamique, le disque de la machine virtuelle conserve le format statique mis à zéro en différé.

- Vous ne pouvez pas chiffrer une machine virtuelle et ses disques à l'aide du menu **Modifier les paramètres**. Vous devez modifier la stratégie de stockage. Il est possible d'effectuer d'autres tâches de chiffrement comme chiffrer un disque non chiffré d'une machine virtuelle chiffrée, à l'aide du menu **Modifier les paramètres** ou en modifiant la stratégie de stockage. Reportez-vous à « Chiffrer une machine ou un disque virtuel existant », page 156.
- Si vous détachez un disque d'une machine virtuelle, les informations sur la stratégie de stockage du disque virtuel ne sont pas conservées.
  - Si le disque virtuel est chiffré, vous devez explicitement définir la stratégie de stockage sur la stratégie de chiffrement des machines virtuelles ou sur une stratégie de stockage qui englobe le chiffrement.
  - Si le disque virtuel n'est pas chiffré, vous pouvez modifier la stratégie de stockage lorsque vous ajoutez le disque à la machine virtuelle.

  Reportez-vous à « Chiffrement des disques virtuels », page 139 pour plus de détails.
- Déchiffrez les vidages de mémoire avant de déplacer une machine virtuelle vers un autre cluster.

  vCenter Server ne stocke pas les clés KMS, mais assure uniquement le suivi des ID de clé. Par conséquent, vCenter Server ne stocke pas la clé de l'hôte ESXi de manière persistante.

  Dans certaines circonstances, par exemple lors du déplacement de l'hôte ESXi vers un autre cluster et du redémarrage de l'hôte, vCenter Server attribue une nouvelle clé d'hôte à l'hôte. Il est impossible de déchiffrer des vidages de mémoire existants avec la nouvelle clé d'hôte.
- L'exportation OVF n'est pas prise en charge pour une machine virtuelle chiffrée.

État de verrouillage des machines virtuelles

Si la clé de la machine virtuelle ou une ou plusieurs clés de disque virtuel sont manquantes, la machine virtuelle passe à l'état verrouillé. Si la machine est à l'état verrouillé, vous ne pouvez pas effectuer ses opérations.

- Si vous chiffrez une machine virtuelle et ses disques à l'aide de vSphere Web Client, la même clé est utilisée pour les deux.
- Lorsque vous effectuez le chiffrement à l'aide de l'API, vous pouvez utiliser différentes clés de chiffrement pour la machine virtuelle et ses disques. Dans ce cas, si vous tentez de mettre sous tension une machine virtuelle et si une des clés de disque est manquante, l'opération de mise sous tension échoue. Pour remédier à cela, retirez le disque virtuel.

Pour obtenir des suggestions de dépannage, reportez-vous à « Résoudre les problèmes de clés manquantes », page 158.

Interopérabilité du chiffrement des machines virtuelles

Le chiffrement des machines virtuelles vSphere comporte des limitations au niveau de la compatibilité avec certains dispositifs et fonctionnalités dans vSphere 6.5.

Vous ne pouvez pas effectuer certaines tâches sur une machine virtuelle chiffrée.

- Pour la plupart des opérations de chiffrement de machines virtuelles, la machine virtuelle doit être mise hors tension. Vous pouvez cloner une machine virtuelle chiffrée et vous pouvez procéder à un rechiffrement superficiel tandis que la machine virtuelle est sous tension.
- Vous ne pouvez pas suspendre ou reprendre une machine virtuelle chiffrée.
- Les opérations de snapshot ont leurs limites.
  - Vous ne pouvez pas cocher la case **Capturer la mémoire de la machine virtuelle** lorsque vous créez un snapshot d'une machine virtuelle chiffrée.

- Il n'est pas possible de chiffrer une machine virtuelle comportant des snapshots existants. Consolidez tous les snapshots existants avant d'effectuer le chiffrement.

Certaines fonctionnalités ne sont pas compatibles avec le chiffrement des machines virtuelles vSphere.

- vSphere Fault Tolerance
- Le clonage est pris en charge.
  - Le clone intégral est pris en charge. Le clone hérite de l'état de chiffrement parent, y compris des clés. Vous pouvez rechiffrer le clone intégral de façon à ce qu'il utilise de nouvelles clés ou vous pouvez déchiffrer le clone intégral.

    Les clones liés sont pris en charge et le clone hérite de l'état de chiffrement parent, y compris des clés. Vous ne pouvez pas déchiffrer le clone lié ou rechiffrer un clone lié avec différentes clés.
- vSphere ESXi Dump Collector
- Migration avec vMotion d'une machine virtuelle chiffrée vers une instance de vCenter Server différente. La migration chiffrée avec vMotion d'une machine virtuelle non chiffrée est prise en charge.
- vSphere Replication
- Bibliothèque de contenu
- Toutes les solutions de sauvegarde reposant sur VMware vSphere Storage API - Data Protection (VADP) pour la sauvegarde de disques virtuels ne sont pas prises en charge.
  - Les solutions de sauvegarde VADP SAN ne sont pas prises en charge.
  - Les solutions d'ajout de sauvegarde à chaud VADP sont prises en charge si le fournisseur prend en charge le chiffrement de la machine virtuelle proxy créée dans le cadre du workflow de sauvegarde. Le fournisseur doit posséder le privilège **Opérations de chiffrement.Chiffrer la machine virtuelle**.
  - Les solutions de sauvegarde VADP NBD-SSL sont prises en charge. L'application du fournisseur doit comporter le privilège **Opérations de chiffrement.Accès direct**.
- Vous pouvez utiliser le chiffrement des machines virtuelles vSphere avec IPv6 en mode mixte mais non dans un environnement purement IPv6. La connexion à un serveur de gestion des clés à l'aide d'une adresse IPv6 uniquement n'est pas prise en charge.
- Vous ne pouvez pas utiliser le chiffrement des machines virtuelles vSphere pour le chiffrement sur d'autres produits VMware tels que VMware Workstation.
- Vous ne pouvez pas envoyer de sortie d'une machine virtuelle chiffrée vers un port en série ou un port parallèle. Même si la configuration semble concluante, la sortie est envoyée vers un fichier.

Certains types de configurations de disque de machine virtuelle ne sont pas pris en charge avec le chiffrement des machines virtuelles vSphere.

- VMware vSphere Flash Read Cache
- Disques de première classe
- RDM (Raw Device Mapping)
- Disques en mode multi-écriture ou disques partagés (MSCS/WSFC/Oracle RAC). Si un disque virtuel est chiffré et si vous tentez de sélectionner le mode multi-écriture dans la page **Modifier les paramètres** de la machine virtuelle, le bouton **OK** est désactivé.

Utiliser le chiffrement dans votre environnement vSphere 7

L'utilisation du chiffrement dans votre environnement vSphere nécessite une certaine préparation. Après avoir configuré votre environnement, vous pouvez créer des machines virtuelles et des disques virtuels chiffrés et chiffrer les machines virtuelles et les disques existants.

Vous pouvez effectuer d'autres tâches à l'aide de l'API et de l'interface de ligne de commande `crypto-util`. Consultez *Guide de programmation de vSphere Web Services SDK* pour obtenir de la documentation sur l'API et l'aide de la ligne de commande `crypto-util` pour plus d'informations sur cet outil.

Ce chapitre aborde les rubriques suivantes :

Configurer le cluster du serveur de gestion des clés

Avant de pouvoir commencer vos tâches de chiffrement de machines virtuelles, vous devez configurer le serveur de gestion des clés (KMS). Cette opération implique d'ajouter le KMS et d'établir une relation de confiance avec celui-ci. Lorsque vous ajoutez un cluster, vous êtes invité à le définir comme cluster par défaut. Vous pouvez modifier explicitement le cluster par défaut. vCenter Server provisionne des clés à partir du cluster par défaut.

KMS doit prendre en charge le protocole KMIP (Key Management Interoperability Protocol) 1.1 standard. Reportez-vous à *Matrices de compatibilité vSphere* pour plus de détails.

Configuration de serveur de gestion des clés de chiffrement de machines virtuelles (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vm_encryption_key_server_setup)

Ajouter un KMS à vCenter Server

L'ajout d'un KMS à votre système vCenter Server se fait depuis vSphere Web Client ou au moyen de l'API publique.

vCenter Server crée un cluster KMS lorsque vous ajoutez la première instance de KMS.

- Lorsque vous ajoutez le KMS, vous êtes invité à définir ce cluster comme valeur par défaut. Vous pouvez ensuite modifier le cluster par défaut de façon explicite.
- Après que vCenter Server crée le premier cluster, vous pouvez ajouter des instances KMS du même fournisseur au cluster.
- Vous ne pouvez configurer le cluster qu'avec une seule instance KMS.
- Si votre environnement prend en charge des solutions KMS de différents fournisseurs, vous pouvez ajouter plusieurs clusters KMS.
- Si votre environnement inclut plusieurs clusters KMS, et si vous supprimez le cluster par défaut, vous devez définir la valeur par défaut de façon explicite. Reportez-vous à « Définir le cluster KMS par défaut », page 152.

Prérequis

- Assurez-vous que le serveur de clés est dans *Matrices de compatibilité vSphere* et est conforme à KMIP 1.1, et qu'il peut être un profil Symmetric Key Foundry And Server.
- Assurez-vous que vous disposez des privilèges requis : **Opérations de chiffrement.Gérer les serveurs de clés**.
- La connexion à un serveur de gestion des clés à l'aide d'une adresse IPv6 uniquement n'est pas prise en charge.

Procédure

1. Connectez-vous au système vCenter Server en utilisant vSphere Web Client.
2. Parcourez la liste d'inventaire et sélectionnez l'instance vCenter Server.
3. Cliquez sur **Configurer**, puis sur **Serveurs de gestion des clés**.
4. Cliquez sur **Ajouter un KMS**, spécifiez les informations KMS dans l'assistant, puis cliquez sur **OK**.

Option	Valeur
Cluster KMS	Sélectionnez **Créer un nouveau cluster** pour créer un nouveau cluster. Si un cluster existe déjà, vous pouvez le sélectionner.
Nom cluster	Nom du cluster KMS. Ce nom peut être nécessaire pour se connecter au KMS si votre instance vCenter Server devient indisponible.
Alias du serveur	Alias du KMS. Cet alias peut être nécessaire pour se connecter au KMS si votre instance vCenter Server devient indisponible.
Adresse du serveur	Adresse IP ou nom de domaine complet du KMS.
Port du serveur	Port sur lequel vCenter Server se connecte au KMS.
Adresse du proxy	Adresse facultative du proxy pour la connexion au KMS.
Port du proxy	Port facultatif du proxy pour la connexion au KMS.

Option	Valeur
Nom d'utilisateur	Certains fournisseurs de KMS permettent aux utilisateurs d'isoler les clés de chiffrement qui sont utilisées par différents utilisateurs ou groupes en spécifiant un nom d'utilisateur et un mot de passe. Ne spécifiez un nom d'utilisateur que si votre KMS prend en charge cette fonctionnalité et si vous avez l'intention de l'utiliser.
Mot de passe	Certains fournisseurs de KMS permettent aux utilisateurs d'isoler les clés de chiffrement qui sont utilisées par différents utilisateurs ou groupes en spécifiant un nom d'utilisateur et un mot de passe. Ne spécifiez un mot de passe que si votre KMS prend en charge cette fonctionnalité et si vous avez l'intention de l'utiliser.

Établir une connexion de confiance en échangeant des certificats

Après avoir ajouté le KMS au système vCenter Server, vous pouvez établir une connexion de confiance. Le détail du processus dépend des certificats que KMS accepte et de la stratégie de l'entreprise.

Prérequis

Ajoutez le cluster KMS.

Procédure

1 Connectez-vous à vSphere Web Client, puis sélectionnez un système vCenter Server.

2 Cliquez sur **Configurer** et sélectionnez **Serveurs de gestion des clés**.

3 Sélectionnez l'instance de KMS avec laquelle vous souhaitez établir une connexion de confiance.

4 Cliquez sur **Établir une relation de confiance avec le KMS**.

5 Sélectionnez l'option correspondant à votre serveur et complétez les étapes requises.

Option	Reportez-vous à
Certificat d'autorité de certification racine	« Utiliser l'option Certificat d'autorité de certification racine pour établir une connexion de confiance », page 149.
Certificat	« Utiliser l'option de certificat pour établir une connexion de confiance », page 150.
Demande de signature du nouveau certificat	« Utiliser l'option Demande de signature du nouveau certificat pour établir une connexion de confiance », page 151.
Télécharger le certificat et la clé privée	« Utiliser l'option Télécharger le certificat et la clé privée pour établir une connexion de confiance », page 151.

Utiliser l'option Certificat d'autorité de certification racine pour établir une connexion de confiance

Certains fournisseurs de KMS comme SafeNet exigent que vous téléchargiez votre certificat d'autorité de certification racine sur le KMS. Tous les certificats qui sont signés par votre autorité de certification racine sont alors approuvés par ce KMS.

Le certificat d'autorité de certification racine que le chiffrement de machines virtuelles vSphere utilise est un certificat autosigné qui est stocké dans un magasin distinct du VECS (VMware Endpoint Certificate Store) sur le système vCenter Server.

Remarque Générez un certificat d'autorité de certification uniquement si vous souhaitez remplacer des certificats existants. Si vous le faites en effet, les autres certificats signés par cette autorité de certification racine deviennent non valides. Vous pouvez générer un nouveau certificat d'autorité de certification racine dans le cadre de ce workflow.

Procédure

1 Connectez-vous à vSphere Web Client, puis sélectionnez un système vCenter Server.

2 Cliquez sur **Configurer** et sélectionnez **Serveurs de gestion des clés**.

3 Sélectionnez l'instance de KMS avec laquelle vous souhaitez établir une connexion de confiance.

4 Sélectionnez **Certificat d'autorité de certification racine** et cliquez sur **OK**.

La boîte de dialogue Télécharger un certificat d'autorité de certification est renseignée avec le certificat racine utilisé par vCenter Server pour le chiffrement. Ce certificat est stocké dans VECS.

5 Copiez le certificat dans le presse-papiers ou téléchargez-le comme un fichier.

6 Suivez les instructions de votre fournisseur de KMS pour télécharger le certificat sur son système.

Remarque Certains fournisseurs de KMS, par exemple SafeNet, exigent que le fournisseur de KMS redémarre le KMS pour détecter le certificat racine que vous téléchargez.

Suivant

Finalisez l'échange de certificat. Reportez-vous à « Terminer la configuration de la confiance », page 152.

Utiliser l'option de certificat pour établir une connexion de confiance

Certains fournisseurs de KMS comme Vormetric exigent que vous téléchargiez le certificat vCenter Server sur le KMS. Une fois le téléchargement effectué, le KMS accepte le trafic provenant d'un système avec ce certificat.

vCenter Server génère un certificat pour protéger les connexions avec le KMS. Le certificat est stocké dans un magasin de clés distinct dans VECS (VMware Endpoint Certificate Store) sur le système vCenter Server.

Procédure

1 Connectez-vous à vSphere Web Client, puis sélectionnez un système vCenter Server.

2 Cliquez sur **Configurer** et sélectionnez **Serveurs de gestion des clés**.

3 Sélectionnez l'instance de KMS avec laquelle vous souhaitez établir une connexion de confiance.

4 Sélectionnez **Certificat** et cliquez sur **OK**.

La boîte de dialogue Télécharger le certificat est renseignée avec le certificat racine utilisé par vCenter Server pour le chiffrement. Ce certificat est stocké dans VECS.

Remarque Ne générez pas de nouveau certificat sauf si vous souhaitez remplacer des certificats existants.

5 Copiez le certificat dans le presse-papier ou téléchargez-le comme un fichier.

6 Suivez les instructions de votre fournisseur de KMS pour mettre à jour le certificat sur le KMS.

Suivant

Finalisez la relation de confiance. Reportez-vous à « Terminer la configuration de la confiance », page 152.

Utiliser l'option Demande de signature du nouveau certificat pour établir une connexion de confiance

Certains fournisseurs de KMS, par exemple Thales, exige que vCenter Server génère un CSR (Certificate Signing Request) et envoie ce CSR au KMS. Le KMS signe le CSR et renvoie le certificat signé. Vous pouvez télécharger le certificat signé sur vCenter Server.

L'utilisation de l'option **Demande de signature du nouveau certificat** se fait en deux étapes. Dans un premier temps, vous générez le CSR et vous l'envoyez au fournisseur de KMS. Vous téléchargez ensuite le certificat signé que vous avez reçu du fournisseur de KMS sur vCenter Server.

Procédure

1 Connectez-vous à vSphere Web Client, puis sélectionnez un système vCenter Server.

2 Cliquez sur **Configurer** et sélectionnez **Serveurs de gestion des clés**.

3 Sélectionnez l'instance de KMS avec laquelle vous souhaitez établir une connexion de confiance.

4 Sélectionnez **Demande de signature du nouveau certificat**, puis cliquez sur **OK**.

5 Dans la boîte de dialogue, copiez dans le presse-papiers le certificat complet de la zone de texte ou téléchargez-le comme un fichier, puis cliquez sur **OK**.

   Utilisez le bouton **Générer un nouveau CSR** dans la zone de dialogue uniquement si vous souhaitez générer explicitement un CSR. L'utilisation de cette option rend les certificats signés basés sur l'ancien CSR non valides.

6 Suivez les instructions fournies par votre fournisseur de KMS pour envoyer le CSR.

7 Lorsque vous recevez le certificat signé du fournisseur de KMS, cliquez de nouveau sur **Serveurs de gestion des clés**, puis sélectionnez une nouvelle fois **Demande de signature du nouveau certificat**.

8 Collez le certificat signé dans la zone de texte du bas ou cliquez sur **Télécharger le fichier** et télécharger le fichier, puis cliquez sur **OK**.

Suivant

Finalisez la relation de confiance. Reportez-vous à « Terminer la configuration de la confiance », page 152.

Utiliser l'option Télécharger le certificat et la clé privée pour établir une connexion de confiance

Certains fournisseurs de KMS comme HyTrust exigent que vous déployiez le certificat du serveur KMS et la clé privée sur le système vCenter Server.

Certains fournisseurs de KMS génèrent un certificat et une clé privée pour la connexion et les mettent à votre disposition. Après le téléchargement des fichiers, le KMS approuve votre instance de vCenter Server.

Prérequis

- Demandez un certificat et une clé privée au fournisseur de KMS. Les fichiers sont des fichiers X509 au format PEM.

Procédure

1 Connectez-vous à vSphere Web Client, puis sélectionnez un système vCenter Server.

2 Cliquez sur **Configurer** et sélectionnez **Serveurs de gestion des clés**.

3 Sélectionnez l'instance de KMS avec laquelle vous souhaitez établir une connexion de confiance.

4 Sélectionnez **Télécharger le certificat et la clé privée** et cliquez sur **OK**.

5 Collez le certificat que vous avez reçu du fournisseur KMS dans la zone de texte du dessus ou cliquez sur **Télécharger le fichier** pour télécharger le fichier de certificat.

6 Collez le fichier de clé dans la zone de texte du dessous ou cliquez sur **Télécharger le fichier** pour télécharger le fichier de clé.

7 Cliquez sur **OK**.

Suivant

Finalisez la relation de confiance. Reportez-vous à « Terminer la configuration de la confiance », page 152.

Définir le cluster KMS par défaut

Vous devez définir le cluster KMS par défaut si vous ne configurez pas le premier cluster comme cluster par défaut, ou si votre environnement utilise plusieurs clusters et que vous supprimez le cluster par défaut.

Prérequis

Nous vous recommandons de vérifier que l'état de la connexion dans l'onglet Serveurs de gestion des clés affiche Normal, ainsi qu'une coche verte.

Procédure

1 Connectez-vous à vSphere Web Client, puis sélectionnez un système vCenter Server.

2 Cliquez sur l'onglet **Configurer**, puis sur **Serveurs de gestion des clés** sous **Plus**.

3 Sélectionnez le cluster et cliquez sur **Définir le cluster KMS comme valeur par défaut**.

Ne sélectionnez pas le serveur. Le menu permettant de définir le cluster par défaut est disponible uniquement pour le cluster.

4 Cliquez sur **Yes**.

Le mot `default` apparaît en regard du nom du cluster.

Terminer la configuration de la confiance

À moins que la boîte de dialogue **Ajouter un serveur** ne vous ait invité à faire confiance au certificat KMS, vous devez explicitement établir la confiance une fois l'échange de certificats terminé.

Vous pouvez terminer la configuration de la confiance, c'est-à-dire indiquer à vCenter Server de faire confiance au certificat KMS, soit en faisant confiance au KMS, soit en téléchargeant un certificat KMS. Deux options s'offrent à vous :

- Faire explicitement confiance au certificat en utilisant l'option **Actualiser le certificat KMS**.
- Télécharger un certificat KMS feuille ou le certificat KMS de l'autorité de certification sur vCenter Server à l'aide de l'option **Télécharger un certificat KMS**.

Remarque Si vous téléchargez le certificat de l'autorité de certification racine ou le certificat de l'autorité de certification intermédiaire, vCenter Server fait confiance à tous les certificats signés par cette autorité de certification. Pour une sécurité renforcée, téléchargez un certificat feuille ou un certificat d'autorité de certification intermédiaire contrôlé par le fournisseur KMS.

Procédure

1 Connectez-vous à vSphere Web Client, puis sélectionnez un système vCenter Server.

2 Cliquez sur **Configurer** et sélectionnez **Serveurs de gestion des clés**.

3 Sélectionnez l'instance de KMS avec laquelle vous souhaitez établir une connexion de confiance.

4 Pour établir la relation de confiance, actualisez ou téléchargez le certificat KMS.

Option	Action
Actualiser le certificat KMS	a Cliquez sur **Toutes les actions** et sélectionnez **Actualiser le certificat KMS**. b Dans la boîte de dialogue qui apparaît, cliquez sur **Faire confiance**.
Télécharger un certificat KMS	a Cliquez sur **Toutes les actions** et sélectionnez **Télécharger le certificat KMS**. b Dans la boîte de dialogue qui s'affiche, cliquez sur **Télécharger le fichier**, téléchargez un fichier de certificat, puis cliquez sur **OK**.

Créer une stratégie de stockage de chiffrement

Avant de pouvoir créer des machines virtuelles chiffrées, vous devez créer une stratégie de stockage de chiffrement. Vous créez la stratégie de stockage une fois, puis vous l'attribuez à chaque fois que vous chiffrez une machine virtuelle ou un disque virtuel.

Si vous souhaitez utiliser le chiffrement de machine virtuelle avec d'autres filtres d'E/S, reportez-vous à la documentation *Stockage vSphere* pour obtenir plus de détails.

Prérequis

- Configurez la connexion au certificat KMS.

  Bien qu'il soit possible de créer une stratégie de stockage de chiffrement de machine virtuelle sans connexion existante au certificat KMS, vous ne pouvez pas effectuer de tâche de chiffrement tant qu'une connexion de confiance n'a pas été établie avec le serveur KMS.

- Privilèges requis : **Opérations cryptographiques.Gérer les stratégies de chiffrement**.

Procédure

1 Connectez-vous à vCenter Server en utilisant vSphere Web Client.

2 Sélectionnez **Accueil**, cliquez sur **Stratégies et profils**, puis cliquez sur **Stratégies de stockage de machine virtuelle**.

3 Cliquez sur **Créer une stratégie de stockage de machine virtuelle**.

4 Spécifiez les valeurs de la stratégie de stockage.

   a Entre un nom de stratégie de stockage et une description facultative, puis cliquez sur **Suivant**.

   b Si vous n'êtes pas familiarisé avec cet assistant, étudiez les informations sur la **Structure de la stratégie**, puis cliquez sur **Suivant**.

   c Cochez la case **Utiliser les règles communes dans la stratégie de stockage de machine virtuelle**.

   d Cliquez sur **Ajouter un composant** et sélectionnez **Chiffrement > Propriétés de chiffrement par défaut**, puis cliquez sur **Suivant**.

   Dans la plupart des cas, les propriétés par défaut sont appropriées. Vous n'aurez besoin d'une stratégie personnalisée que si vous souhaitez associer le chiffrement à d'autres fonctionnalités telles que la mise en cache ou la réplication.

   e Décochez la case **Utiliser les ensembles de règles dans la stratégie de stockage** et cliquez sur **Suivant**.

   f Sur la page Compatibilité du stockage, laissez l'option Compatible sélectionnée, sélectionnez une banque de données, puis cliquez sur **Suivant**.

   g Passez vos informations en revue et cliquez sur **Terminer**.

Activer explicitement le mode de chiffrement de l'hôte

Le mode de chiffrement de l'hôte doit être activé si vous souhaitez effectuer des tâches de chiffrement, par exemple pour créer une machine virtuelle chiffrée sur un hôte ESXi. Dans la plupart des cas, le mode de chiffrement de l'hôte est automatiquement activé lorsque vous effectuez une tâche de chiffrement.

Dans certains cas, il est nécessaire d'activer explicitement le mode de chiffrement. Reportez-vous à « Conditions préalables et privilèges requis pour les tâches de chiffrement », page 140.

Prérequis

Privilège requis : **Cryptographic operations.Register host**

Procédure

1 Pour activer le mode de chiffrement de l'hôte, procédez comme suit.

2 Connectez-vous à vCenter Server à l'aide de vSphere Web Client.

3 Sélectionnez l'hôte ESXi et cliquez sur **Configurer**.

4 Dans Système, cliquez sur **Profil de sécurité**.

5 Faites défiler la liste jusqu'à l'option Mode de chiffrement de l'hôte et cliquez sur **Modifier**.

6 Sélectionnez **Activé** et cliquez sur **OK**.

Désactiver le mode de chiffrement de l'hôte

Le mode de chiffrement de l'hôte est automatiquement activé lorsque vous effectuez une tâche de chiffrement. Une fois le mode de chiffrement de l'hôte activé, tous les vidages de mémoire sont chiffrés afin d'éviter que des informations sensibles ne soient communiquées au personnel d'assistance. Si vous n'utilisez plus le chiffrement de machine virtuelle avec un hôte ESXi, vous pouvez désactiver le mode de chiffrement.

Procédure

1 Annuler l'enregistrement de toutes les machines virtuelles chiffrées auprès de l'hôte

2 Annulez l'enregistrement de l'hôte auprès de vCenter Server.

3 Redémarrez l'hôte.

4 Enregistrez à nouveau l'hôte auprès de vCenter Server.

Le mode de chiffrement de l'hôte demeure désactivé tant que vous n'ajoutez pas de machines virtuelles chiffrées.

Créer une machine virtuelle chiffrée

Une fois le KMS configuré, vous pouvez créer des machines virtuelles chiffrées. Les nouvelles machines virtuelles créées au moyen d'une stratégie de stockage de chiffrement sont chiffrées automatiquement.

Remarque La création d'une machine virtuelle chiffrée est plus rapide et consomme moins de ressources de stockage que le chiffrement d'une machine virtuelle existante. Chiffrez la machine virtuelle dans le cadre du processus de création, si possible.

Prérequis

- Établissez une connexion de confiance avec le serveur KMS et sélectionnez un serveur KMS par défaut.
- Créez une stratégie de stockage de chiffrement.

- Assurez-vous que la machine virtuelle est hors tension.
- Vérifiez que vous disposez des privilèges requis.
  - **Opérations de chiffrement.Chiffrer un nouvel élément**
  - Si le mode de chiffrement de l'hôte n'est pas Activé, vous devez également **Opérations de chiffrement.Enregistrer un hôte**.

Procédure

1 Connectez-vous à vCenter Server à l'aide de vSphere Web Client.

2 Sélectionnez un objet dans l'inventaire qui est un objet parent valide d'une machine virtuelle, par exemple un hôte ESXi ou un cluster.

3 Cliquez avec le bouton droit sur, sélectionnez **Nouvelle machine virtuelle > Nouvelle machine virtuelle** et suivez les invites pour créer une machine virtuelle chiffrée.

Option	Action
Sélectionner un type de création	Créez une machine virtuelle.
Sélectionner un nom et un dossier	Spécifiez un nom et un emplacement cible
Sélectionner une ressource de calcul	Spécifiez un objet pour lequel vous avez des privilèges de création de machines virtuelles. Reportez-vous à « Conditions préalables et privilèges requis pour les tâches de chiffrement », page 140.
Sélectionner le stockage	Dans la stratégie de stockage de la machine virtuelle, sélectionnez la stratégie de stockage de chiffrement. Sélectionnez une banque de données compatible.
Sélectionner une compatibilité	Sélectionnez la compatibilité. Vous ne pouvez faire migrer une machine virtuelle chiffrée que sur les hôtes compatibles avec ESXi 6.5 ou une version plus récente.
Sélectionner un système d'exploitation client	Sélectionnez le système d'exploitation invité sur lequel vous prévoyez d'installer ultérieurement la machine virtuelle.
Personnalisation du matériel	Personnalisez le matériel. Par exemple, changez la taille du disque ou le CPU. Tout nouveau disque dur créé est chiffré. Vous pouvez modifier la stratégie de stockage de certains disques par la suite, si nécessaire.
Prêt à terminer	Passez vos informations en revue et cliquez sur **Terminer**.

Cloner une machine virtuelle chiffrée

Lors du clonage d'une machine virtuelle chiffrée, le clone est chiffré avec les mêmes clés. Pour modifier les clés du clone, arrêtez ce dernier et procédez à un rechiffrement superficiel du clone au moyen de l'API. Reportez-vous à *Guide de programmation de vSphere Web Services SDK*.

Il n'est pas nécessaire de mettre la machine virtuelle hors tension pour la cloner.

Prérequis

- Établissez une connexion de confiance avec le serveur KMS et sélectionnez un serveur KMS par défaut.
- Créez une stratégie de stockage de chiffrement.
- Privilèges requis :
  - **Opérations de chiffrement.Cloner**
  - Si le mode de chiffrement de l'hôte n'est pas Activé, vous devez également disposer de privilèges **Opérations de chiffrement.Enregistrer un hôte**.

Procédure

1 Connectez-vous à vCenter Server à l'aide de vSphere Web Client.

2 Sélectionnez un objet dans l'inventaire qui est un objet parent valide d'une machine virtuelle, par exemple un hôte ESXi ou un cluster.

3 Cliquez avec le bouton droit sur la machine virtuelle et suivez les invites pour créer le clone d'une machine virtuelle chiffrée.

Option	Action
Sélectionner un nom et un dossier	Indiquez le nom et l'emplacement cible du clone.
Sélectionner une ressource de calcul	Spécifiez un objet pour lequel vous avez des privilèges de création de machines virtuelles. Reportez-vous à « Conditions préalables et privilèges requis pour les tâches de chiffrement », page 140.
Sélectionner le stockage	Effectuez une sélection dans le menu **Sélectionner un format de disque virtuel** et sélectionnez une banque de données. Vous ne pouvez pas modifier la stratégie de stockage dans le cadre de l'opération de clonage.
Sélectionner les options du clone	Sélectionnez des options de clone, comme abordé dans la documentation de *Administration d'une machine virtuelle vSphere*.
Prêt à terminer	Passez vos informations en revue et cliquez sur **Terminer**.

Chiffrer une machine ou un disque virtuel existant

Vous pouvez chiffrer une machine ou un disque virtuel existant en modifiant sa stratégie de stockage. Vous ne pouvez chiffrer les disques virtuels que pour les machines virtuelles qui sont elles-mêmes chiffrées.

Vous ne pouvez pas chiffrer une machine virtuelle depuis le menu **Modifier les paramètres**. Vous pouvez chiffrer les disques virtuels d'une machine virtuelle chiffrée avec le menu **Modifier les paramètres**.

Prérequis

- Établissez une connexion de confiance avec le serveur KMS et sélectionnez un serveur KMS par défaut.
- Créez une stratégie de stockage de chiffrement.
- Assurez-vous que la machine virtuelle est hors tension.
- Vérifiez que vous disposez des privilèges requis.
  - **Opérations de chiffrement.Chiffrer un nouvel élément**
  - Si le mode de chiffrement de l'hôte n'est pas Activé, vous devez également **Opérations de chiffrement.Enregistrer un hôte**.

Procédure

1 Connectez-vous à vCenter Server à l'aide de vSphere Web Client.

2 Cliquez avec le bouton droit sur la machine virtuelle à modifier et sélectionnez **Stratégies de VM > Modifier les stratégies de stockage VM**.

Vous pouvez définir la stratégie de stockage des fichiers de machines virtuelles, représentée par Accueil VM, ainsi que la stratégie de stockage des disques virtuels.

3 Sélectionnez la stratégie de stockage à utiliser dans le menu déroulant.

- Pour chiffrer la machine virtuelle et ses disques durs, sélectionnez une stratégie de stockage de chiffrement, et cliquez sur **Appliquer à tous**.
- Pour chiffrer la machine virtuelle sans chiffrer les disques virtuels, sélectionnez la stratégie de stockage de chiffrement pour Accueil VM et les autres stratégies de stockage des disques virtuels, puis cliquez sur **Appliquer**.

Vous ne pouvez pas chiffrer le disque virtuel d'une machine virtuelle non chiffrée.

4 (Facultatif) Si vous le préférez, vous pouvez chiffrer les disques virtuels depuis le menu **Modifier les paramètres**.

a Cliquez avec le bouton droit sur la machine virtuelle et sélectionnez **Modifier les paramètres**.

b Laissez l'option **Matériel virtuel** sélectionnée.

c Ouvrez le disque virtuel pour lequel vous souhaitez modifier la stratégie de stockage et sélectionnez une entrée dans le menu déroulant **Stratégie de stockage VM**.

d Cliquez sur **OK**.

Déchiffrer une machine ou un disque virtuel

Vous pouvez déchiffrer une machine virtuelle en modifiant sa stratégie de stockage.

Toutes les machines virtuelles chiffrées nécessitent le paramètre vMotion chiffré. Pendant le processus de déchiffrement des machines virtuelles, le paramètre vMotion chiffré demeure. Vous devez modifier ce paramètre de façon explicite, afin que l'option VMotion chiffré ne soit plus utilisée.

Cette tâche explique comment procéder au déchiffrement au moyen des stratégies de stockage. Avec les disques virtuels, vous pouvez également procéder au déchiffrement depuis le menu **Modifier les paramètres**.

Prérequis

- La machine virtuelle doit être chiffrée.
- La machine virtuelle doit être hors tension ou en mode de maintenance.
- Privilèges requis : **Opérations de chiffrement.Déchiffrer**

Procédure

1 Connectez-vous à vCenter Server à l'aide de vSphere Web Client.

2 Cliquez avec le bouton droit sur la machine virtuelle à modifier et sélectionnez **Stratégies de VM > Modifier les stratégies de stockage VM**.

Vous pouvez définir la stratégie de stockage des fichiers de machines virtuelles, représentée par Accueil VM, ainsi que la stratégie de stockage des disques virtuels.

3 Sélectionnez une stratégie de stockage dans le menu déroulant.

- Pour déchiffrer la machine virtuelle et ses disques durs, cliquez sur **Appliquer à tous**.
- Pour déchiffrer un disque virtuel, mais pas la machine virtuelle, sélectionnez la stratégie de stockage du disque virtuel dans le menu déroulant de la table. Ne modifiez pas la stratégie d'Accueil VM.

Vous ne pouvez pas déchiffrer la machine virtuelle et laisser le disque dur chiffré.

4 Cliquez sur **OK**.

5 (Facultatif) Vous pouvez désormais modifier le paramètre VMotion chiffré.

a Cliquez avec le bouton droit sur la machine virtuelle et cliquez sur**Modifier les paramètres**.

b Cliquez sur **Options VM** et ouvrez la section **Chiffrement**.

c Définissez la valeur de **vMotion chiffré**.

Modifier la stratégie de chiffrement des disques virtuels

Lorsque vous créez une machine virtuelle chiffrée depuis vSphere Web Client, tous les disques virtuels que vous ajoutez pendant le processus de création sont chiffrés. Vous pouvez déchiffrer des disques virtuels avec l'option **Modifier les stratégies de stockage VM**.

Remarque Une machine virtuelle chiffrée peut comporter des disques virtuels qui ne sont pas chiffrés. Cependant, une machine virtuelle chiffrée ne peut pas avoir de disques virtuels chiffrés.

Reportez-vous à « Chiffrement des disques virtuels », page 139.

Cette tâche explique comment modifier la stratégie de chiffrement au moyen des stratégies de stockage. Vous pouvez également utiliser le menu **Modifier les paramètres** pour effectuer cette modification.

Prérequis

Vous devez avoir le privilège **Opérations de chiffrement.Gérer les stratégies de chiffrement**.

Procédure

1 Cliquez avec le bouton droit sur la machine virtuelle dans vSphere Web Client et sélectionnez **Stratégies de VM > Modifier les stratégies de stockage VM**.

2 Sélectionnez le disque dur pour lequel vous souhaitez modifier la stratégie de stockage et sélectionnez la stratégie voulue, par exemple Valeur par défaut de la banque de données.

Résoudre les problèmes de clés manquantes

Si l'hôte ESXi ne parvient pas à obtenir la clé (KEK) pour une machine virtuelle chiffrée ou pour un disque virtuel chiffré de vCenter Server, vous pouvez toujours annuler l'enregistrement ou recharger la machine virtuelle. Vous ne pouvez pas effectuer d'autres opérations de machine virtuelle comme la suppression de la machine virtuelle ou la mise sous tension de la machine virtuelle. La machine virtuelle est verrouillée.

Si la clé de la machine virtuelle n'est pas disponible, l'état de la machine virtuelle dans vSphere Web Client s'affiche comme non valide et la machine virtuelle ne peut pas être mise sous tension. Si la clé de la machine virtuelle est disponible, mais qu'une clé pour un disque chiffré n'est pas disponible, l'état de la machine virtuel ne s'affiche pas comme non valide, mais la machine virtuelle ne peut pas être mise sous tension et l'erreur suivante se produit :

```
The disk [/path/to/the/disk.vmdk] is encrypted and no password was provided.
```

Procédure

1 Si le problème concerne la connexion entre le système vCenter Server et KMS, restaurez la connexion.

Si KMS n'est pas disponible, les machines virtuelles sont déverrouillées.

2 Si la connexion est restaurée et qu'une erreur se produit lorsque vous tentez d'enregistrer la machine virtuelle, vérifiez que vous disposez du privilège **Opérations de chiffrement.Gérer les clés** pour le système vCenter Server.

Ce privilège n'est pas nécessaire à la mise sous tension d'une machine virtuelle chiffrée si la clé est disponible, mais il est requis pour enregistrer la machine virtuelle dans le cas où la clé doit être récupérée de nouveau.

3 Si la clé n'est plus active sur KMS, demandez à l'administrateur KMS de restaurer la clé.

Ceci peut se produire si vous mettez sous tension une machine virtuelle qui a été supprimée de l'inventaire et qui n'a pas été enregistrée depuis longtemps. Cela se produit également si vous redémarrez l'hôte ESXi et que KMS n'est pas disponible.

a Récupérez l'ID de la clé en utilisant Managed Object Browser (MOB) ou vSphere API.

Récupérez l'`keyId` de `VirtualMachine.config.keyId.keyId`.

b Demandez à l'administrateur KMS de réactiver la clé qui est associée à cet ID de clé.

Si la clé peut être restaurée sur KMS, vCenter Server la récupère et la transmet à l'hôte ESXi dès que celui-ci en a besoin.

4 Si KMS est accessible et que l'hôte ESXi est mis sous tension, mais que le système vCenter Server n'est pas disponible, suivez ces étapes pour déverrouiller les machines virtuelles.

a Restaurez le système vCenter Server ou configurez un système vCenter Server différent en tant que client KMS.

Vous devez utiliser le même nom de cluster, mais l'adresse IP peut être différente.

b Réenregistrez toutes les machines virtuelles qui sont verrouillées.

La nouvelle instance de vCenter Server récupère les clés de KMS et les machines virtuelles sont déverrouillées.

Chiffrement de machines virtuelles vSphere et vidages mémoire

Si votre environnement utilise le chiffrement de machines virtuelles vSphere et si une erreur se produit sur l'hôte ESXi, le vidage mémoire qui en résulte est chiffré pour protéger les données clients. Les vidages mémoire qui sont inclus dans le module vm-support sont également chiffrés.

Remarque Les vidages de mémoire peuvent contenir des informations sensibles. Suivez la politique de votre organisation en matière de sécurité et de confidentialité lorsque vous gérez des vidages mémoire.

Vidages mémoire sur hôtes ESXi

Lorsqu'un hôte ESXi se bloque et que le mode de chiffrement est activé pour cet hôte, un vidage mémoire chiffré est généré et l'hôte redémarre. Le vidage mémoire est chiffré avec la clé de l'hôte qui se trouve dans le cache de la clé ESXi. Ce que vous pouvez faire ensuite dépend de plusieurs facteurs.

- Dans la plupart des cas, vCenter Server récupère la clé de l'hôte à partir du KMS et tente de transmettre la clé à l'hôte ESXi après le redémarrage. Si l'opération réussit, vous pouvez générer le module vm-support et vous pouvez déchiffrer ou rechiffrer le vidage mémoire. Reportez-vous à « Déchiffrer ou chiffrer à nouveau un vidage de mémoire chiffré », page 161.
- Si vCenter Server ne peut pas se connecter à l'hôte ESXi, vous devriez pouvoir récupérer la clé du KMS. Reportez-vous à « Résoudre les problèmes de clés manquantes », page 158.
- Si l'hôte a utilisé une clé personnalisée et que cette clé diffère de la clé que vCenter Server transmet à l'hôte, vous ne pouvez pas manipuler le vidage mémoire. Évitez d'utiliser des clés personnalisées.

Vidages mémoire et modules vm-support

Lorsque vous contactez le support technique de VMware pour une erreur grave, votre représentant du support vous demande généralement de générer un module vm-support. Le module inclut des fichiers journaux et d'autres informations, notamment les vidages mémoire. Si votre représentant du support ne parvient pas à résoudre les problèmes en examinant les fichiers journaux et les autres informations, il peut

vous demander de déchiffrer les vidages mémoire et de lui transmettre les informations pertinentes. Suivez la politique de votre organisation en matière de sécurité et de confidentialité pour protéger les informations sensibles comme les clés des hôtes. Reportez-vous à « Collecter un module vm-support pour un hôte ESXi qui utilise le chiffrement », page 160.

Vidages mémoire sur systèmes vCenter Server

Un vidage mémoire sur un système vCenter Server n'est pas chiffré. vCenter Server contient déjà des informations potentiellement sensibles. Assurez-vous au minimum que le système Windows sur lequel vCenter Server s'exécute ou que l'instance de vCenter Server Appliance est protégée. Reportez-vous à Chapitre 4, « Sécurisation des systèmes vCenter Server », page 107. Il peut également s'avérer utile de désactiver les vidages mémoire pour le système vCenter Server. Les autres informations contenues dans les fichiers journaux peuvent aider à déterminer le problème.

Collecter un module vm-support pour un hôte ESXi qui utilise le chiffrement

Si le mode de chiffrement de l'hôte est activé pour l'ESXi, tout vidage de mémoire intervenant dans le module `vm-support` est chiffré. Vous pouvez collecter le module auprès de vSphere Web Client. Vous pouvez également spécifier un mot de passe si vous prévoyez de déchiffrer le vidage de mémoire à une date ultérieure.

Le module `vm-support` inclut des fichiers journaux, des fichiers de vidage de mémoire, etc.

Prérequis

Informez votre représentant de l'assistance technique que le mode de chiffrement de l'hôte est activé pour l'hôte ESXi. Votre représentant de l'assistance technique vous demandera peut-être de déchiffrer les vidages de mémoire et d'extraire les informations appropriées.

Remarque Les vidages de mémoire peuvent contenir des informations sensibles. Suivez la politique de votre organisation en matière de sécurité et de confidentialité pour protéger les informations sensibles comme les clés des hôtes.

Procédure

1. Connectez-vous au système vCenter Server en utilisant vSphere Web Client.
2. Cliquez sur **Hôtes et clusters**, puis cliquez avec le bouton droit de la souris sur l'hôte ESXi.
3. Sélectionnez l'option **Exporter les journaux système**.
4. Dans la boîte de dialogue, sélectionnez l'option **Mot de passe pour les vidages de mémoire chiffrés**, puis indiquez un mot de passe et confirmez-le.
5. Pour les autres options, conservez les paramètres par défaut ou effectuez des modifications si l'assistance technique VMware vous y invite, puis cliquez sur **Terminer**.
6. Indiquez l'emplacement du fichier.
7. Si votre représentant de l'assistance technique vous a demandé de déchiffrer le vidage de mémoire dans le module `vm-support`, connectez-vous à n'importe quel hôte ESXi et appliquez la procédure suivante.
   a. Connectez-vous à l'ESXi, puis au répertoire dans lequel se trouve le module `vm-support`.

      Le nom de fichier est de type esx.date_et_heure.tgz.

   b. Assurez-vous que le répertoire dispose de suffisamment d'espace pour le module, le module décompressé et le module recompressé, ou déplacez le module.

c Procédez à l'extraction du module dans le répertoire local.

```
vm-support -x *.tgz .
```

La hiérarchie de fichiers qui en résulte peut contenir des fichiers de vidage de mémoire pour l'hôte ESXi, en général dans `/var/core`. Elle peut contenir plusieurs fichiers de vidage de mémoire pour des machines virtuelles.

d Déchiffrez individuellement chaque fichier de vidage de mémoire chiffré.

```
crypto-util envelope extract --offset 4096 --keyfile vm-support-incident-key-file
--password encryptedZdump decryptedZdump
```

vm-support-incident-key-file est le fichier de clé d'incident se trouvant au niveau supérieur du répertoire.

encryptedZdump est le nom du fichier de vidage de mémoire chiffré.

decryptedZdump est le nom du fichier généré par la commande. Rendez le nom semblable à celui du fichier *encryptedZdump*.

e Fournissez le mot de passe que vous avez spécifié lors de la création du module `vm-support`.

f Supprimez les vidages de mémoire chiffrés et compressez à nouveau le module.

```
vm-support --reconstruct
```

8 Supprimez tout fichier contenant des informations confidentielles.

Déchiffrer ou chiffrer à nouveau un vidage de mémoire chiffré

Vous pouvez déchiffrer, ou chiffrer à nouveau, un vidage de mémoire chiffré sur votre hôte ESXi à l'aide de l'interface de ligne de commande `crypto-util`.

Vous pouvez vous-même déchiffrer et examiner les vidages de mémoire dans le module vm-support. Le vidage de mémoire peut contenir des informations sensibles. Suivez la politique de votre organisation en matière de sécurité et de confidentialité pour protéger les informations sensibles comme les clés des hôtes.

Pour plus de détails sur le rechiffrement d'un vidage de mémoire et sur d'autres fonctionnalités de `crypto-util`, consultez l'aide de la ligne de commande.

Remarque `crypto-util` est destinée à des utilisateurs expérimentés.

Prérequis

La clé d'hôte ESXi ayant servi à chiffrer le vidage de mémoire doit être disponible sur l'hôte ESXi qui a généré le vidage de mémoire.

Procédure

1 Connectez-vous directement à l'hôte ESXi sur lequel le vidage de mémoire s'est produit.

Si l'hôte ESXi est en mode de verrouillage, ou si l'accès SSH est désactivé, vous devrez peut-être commencer par activer l'accès.

2 Déterminez si le vidage de mémoire est chiffré.

Option	Description
Surveiller le vidage de mémoire	`crypto-util envelope describe vmmcores.ve`
fichier zdump	`crypto-util envelope describe --offset 4096 zdumpFile`

3 Déchiffrez le vidage de mémoire; selon son type.

Option	Description
Surveiller le vidage de mémoire	`crypto-util envelope extract vmmcores.ve vmmcores`
fichier zdump	`crypto-util envelope extract --offset 4096` *zdumpEncrypted zdumpUnencrypted*

Sécurisation de la mise en réseau vSphere 8

La sécurisation de la mise en réseau vSphere constitue une part essentielle de la protection de votre environnement. Vous sécurisez différents composants vSphere de différentes manières. Pour plus d'informations sur la mise en réseau dans l'environnement vSphere, reportez-vous à la documentation *Mise en réseau vSphere*.

Ce chapitre aborde les rubriques suivantes :

Introduction à la sécurité du réseau vSphere

La sécurité du réseau dans l'environnement vSphere partage de nombreuses caractéristiques de sécurisation d'un environnement de réseau physique, mais inclut également des caractéristiques qui s'appliquent uniquement aux machines virtuelles.

Pare-feu

Ajoutez une protection par pare-feu à votre réseau virtuel en installant et en configurant des pare-feu hébergés sur hôte sur certaines ou la totalité de ses machines virtuelles.

Pour une plus grand efficacité, vous pouvez configurer des réseaux Ethernet privés de machines virtuelles ou des réseaux virtuels. Avec les réseaux virtuels, vous installez un pare-feu hébergé sur hôte sur une machine virtuelle à la tête du réseau virtuel. Ce pare-feu sert de tampon de protection entre l'adaptateur réseau physique et les machines virtuelles restantes du réseau virtuel.

Étant donné que les pare-feu hébergés sur hôte peuvent ralentir les performances, équilibrez vos besoins en sécurité par rapport aux objectifs de performances avant d'installer des pare-feu hébergés sur hôte sur des machines virtuelles ailleurs dans le réseau virtuel.

Reportez-vous à la section « Sécurisation du réseau avec des pare-feu », page 164.

Segmentation

Conservez différentes zones de machines virtuelles au sein d'un hôte sur différents segments du réseau. Si vous isolez chaque zone de machines virtuelles sur leur propre segment de réseau, vous réduisez le risque de fuite de données d'une zone de machines virtuelles à la suivante. La segmentation empêche diverses menaces, y compris l'usurpation d'adresse ARP (Address Resolution Protocol), dans laquelle un attaquant manipule la table ARP pour remapper les adresses MAC et IP, obtenant ainsi accès au trafic réseau de et vers un hôte. Les pirates utilisent la falsification de la réponse ARP (ARP spoofing) pour générer des attaques « Man in the Middle » (MITM), effectuer des attaques par déni de service (DoS), pirater le système cible ou perturber le réseau virtuel.

La planification soignée de la segmentation réduit les chances de transmissions de paquets entre les zones de machines virtuelles, ce qui empêche les attaques de reniflement qui nécessitent l'envoi de trafic réseau à la victime. Par conséquent, un attaquant ne peut pas utiliser un service non sécurisé sur une zone de machines virtuelles pour accéder aux autres zones de machines virtuelles de l'hôte. Vous pouvez implémenter la segmentation à l'aide de l'une des deux approches suivantes, chacune d'entre elles ayant des avantages différents.

- Utilisez des adaptateurs réseau physiques séparés pour des zones de machines virtuelles afin de garantir que les zones sont isolées. Conserver des adaptateurs réseau physiques séparés pour des zones de machines virtuelles est probablement la méthode la plus sécurisée et moins susceptible de subir une configuration incorrecte après la création des segments initiaux.
- Configurez des réseaux locaux virtuels (VLAN) pour protéger votre réseau. Comme les VLAN disposent de presque tous les avantages de sécurité inhérents à l'implémentation de réseaux séparés physiquement sans surcharge matérielle, ils offrent une solution viable pouvant vous économiser les coûts de déploiement et d'entretien de périphériques, câblages, etc. supplémentaires. Reportez-vous à la section « Sécurisation des machines virtuelles avec des VLAN », page 172.

Prévention de l'accès non autorisé

Si votre réseau de machines virtuelles est connecté à un réseau physique, il peut être soumis à des défaillances tout comme un réseau constitué de machines physiques. Même si le réseau de machines virtuelles est isolé de tout réseau physique, les machines virtuelles du réseau peuvent être soumises à des attaques d'autres machines virtuelles du réseau. Les contraintes de sécurisation des machines virtuelles sont souvent identiques à celles des machines physiques.

Les machines virtuelles sont isolées les unes des autres. Une machine virtuelle ne peut pas lire ou écrire sur la mémoire d'une autre machine virtuelle, accéder à ses données, utiliser ses applications, etc. Cependant, dans le réseau, toute machine virtuelle ou groupes de machines virtuelles peut toujours être la cible d'un accès non autorisé à partir d'autres machines virtuelles et peut nécessiter une protection supplémentaire par des moyens externes.

Sécurisation du réseau avec des pare-feu

Les administrateurs de sécurité utilisent des pare-feu pour protéger le réseau ou les composants sélectionnés dans le réseau des intrusions.

Les pare-feu contrôlent l'accès aux périphériques dans leur périmètre en fermant tous les ports, excepté pour ceux que l'administrateur désigne explicitement ou implicitement comme autorisés. Les ports que les administrateurs ouvrent permettent le trafic entre les périphériques sur différents côtés du pare-feu.

Important Le pare-feu ESXi d'ESXi 5.5 et versions ultérieures n'autorise pas le filtrage par réseau du trafic vMotion. Par conséquent, vous devez établir des règles sur votre pare-feu externe pour vous assurer qu'aucune connexion entrante ne peut être réalisée vers le socket vMotion.

Dans un environnement de machines virtuelles, vous pouvez planifier la disposition des pare-feu entre les composants.

- Pare-feu entre machines physiques telles que des systèmes vCenter Server et des hôtes ESXi.
- Pare-feu entre une machine virtuelle et une autre, par exemple entre une machine virtuelle agissant comme serveur Web externe et une machine virtuelle connectée au réseau interne de votre entreprise.
- Pare-feu entre une machine physique et une machine virtuelle, par exemple lorsque vous placez un pare-feu entre une carte réseau physique et une machine virtuelle.

L'utilisation des pare-feu dans une configuration ESXi dépend de la manière dont vous planifiez l'utilisation du réseau et du niveau de sécurité dont certains composants ont besoin. Par exemple, si vous créez un réseau virtuel où chaque machine virtuelle est dédiée à l'exécution d'une suite de tests de référence différents pour le même service, le risque d'accès non autorisé d'une machine virtuelle à une autre est minime. Par conséquent, une configuration où des pare-feu sont présents entre les machines virtuelles n'est pas nécessaire. Cependant, pour empêcher l'interruption d'un test exécuté à partir d'un hôte externe, vous pouvez configurer un pare-feu au point d'entrée du réseau virtuel pour protéger tout l'ensemble de machines virtuelles.

Pour un diagramme des ports de pare-feu, reportez-vous à l'article 2131180 de la base de connaissances VMware.

Pare-feu pour les configurations avec vCenter Server

Si vous accédez aux hôtes ESXi par l'intermédiaire de vCenter Server, vous protégez généralement vCenter Server à l'aide d'un pare-feu.

Des pare-feu doivent être présents aux points d'entrée. Un pare-feu peut être situé entre les clients et vCenter Server ou vCenter Server et les clients peuvent être situés derrière le pare-feu.

Pour obtenir la liste complète des ports TCP et UDP, reportez-vous aux sections « Ports requis pour vCenter Server et l'instance de Platform Services Controller », page 114 et « Ports TCP et UDP supplémentaires pour vCenter Server », page 119.

Les réseaux configurés avec vCenter Server peuvent recevoir les communications par le biais de vSphere Web Client, de l'interface utilisateur des autres clients ou des clients qui utilisent vSphere API. Pendant le fonctionnement normal, vCenter Server écoute les données de ses hôtes et clients gérés sur les ports désignés. vCenter Server suppose aussi que ces hôtes gérés écoutent les donnés de vCenter Server sur les ports désignés. Si un pare-feu est présent entre l'un de ces éléments, vous devez vous assurer que le pare-feu a des ports ouverts pour prendre en charge le transfert des données.

Vous pouvez également inclure des pare-feu aux autres points d'accès dans le réseau, en fonction de l'utilisation du réseau et du niveau de sécurité requis par les clients. Sélectionnez les emplacements de vos pare-feu en fonction des risques de sécurité pour la configuration de votre réseau. Les emplacements de pare-feu suivants sont généralement utilisés.

- Entre vSphere Web Client ou un client de gestion de réseau tiers et vCenter Server.
- Si vos utilisateurs accèdent aux machines virtuelles via un navigateur Web, entre le navigateur Web et l'hôte ESXi.
- Si vos utilisateurs accèdent à des machines virtuelles par l'intermédiaire de vSphere Web Client, entre vSphere Web Client et l'hôte ESXi. Cette connexion s'ajoute à la connexion entre vSphere Web Client et vCenter Server et elle nécessite un port différent.
- Entre vCenter Server et les hôtes ESXi.
- Entre les hôtes ESXi de votre réseau. Bien que le trafic entre les hôtes soit généralement considéré comme sécurisé, vous pouvez ajouter des pare-feu entre eux si vous vous inquiétez des défaillances de sécurité de machine à machine.

Si vous ajoutez des pare-feu entre les hôtes ESXi et que vous prévoyez de migrer des machines virtuelles entre elles, ouvrez les ports dans les pare-feu qui séparent l'hôte source des hôtes cibles.

- Entre les hôtes ESXi et le stockage réseau tel que le stockage NFS ou iSCSI. Ces ports ne sont pas spécifiques à VMware et vous pouvez les configurer en fonction des spécifications de votre réseau.

Connexion à vCenter Server via un pare-feu

vCenter Server utilise par défaut le port TCP 443 pour surveiller les transferts de données à partir de ses clients. Si vous disposez d'un pare-feu placé entre vCenter Server et ses clients, vous devez configurer la connexion par l'intermédiaire de laquelle vCenter Server peut recevoir des données des clients.

Ouvrez le port TCP 443 dans le pare-feu pour permettre à vCenter Server de recevoir des données. La configuration du pare-feu dépend de ce qui est utilisé sur votre site. Renseignez-vous auprès de l'administrateur système de votre pare-feu local.

Si vous ne souhaitez pas utiliser le port 443 pour la communication vSphere Web Client vers vCenter Server, vous pouvez basculer sur un autre port. La manière dont vous ouvrez le port varie selon que vous utilisez un dispositif vCenter Server Appliance ou une installation sous Windows de vCenter Server.

Si vous utilisez toujours VMware Host Client, reportez-vous à la documentation *Gestion individuelle des hôtes vSphere - VMware Host Client*.

Pare-feu pour les configurations sans vCenter Server

Vous pouvez connecter les clients directement à votre réseau ESXi si votre environnement n'inclut pas vCenter Server.

Les hôtes autonomes reçoivent des communications via VMware Host Client, l'une des interfaces de ligne de commande de vSphere, vSphere Web Services SDK ou des clients tiers. Les exigences de pare-feu pour les hôtes autonomes sont similaires aux exigences lorsque vCenter Server est présent.

- Utilisez un pare-feu pour protéger votre couche ESXi ou, en fonction de votre configuration, vos clients et la couche ESXi. Ce pare-feu fournit une protection de base à votre réseau.
- La licence pour ce type de configuration fait partie du module ESXi que vous installez sur chacun des hôtes. L'attribution de licence étant résidente dans ESXi, un serveur de licence distinct avec un pare-feu n'est pas nécessaire.

Vous pouvez configurer les ports du pare-feu à l'aide d'ESXCLI ou VMware Host Client. Voir *Gestion individuelle des hôtes vSphere - VMware Host Client*.

Connexion des hôtes ESXi via des pare-feu

Si vous avez un pare-feu entre les hôtes ESXi et vCenter Server, assurez-vous que les hôtes gérés peuvent recevoir des données.

Pour configurer une connexion pour recevoir des données, ouvrez les ports au trafic des services tels que vSphere High Availability, vMotion, et vSphere Fault Tolerance. Reportez-vous à « ESXi », page 67 pour consulter une description des fichiers de configuration, de l'accès à vSphere Web Client et des commandes de pare-feu. Reportez-vous à « Ports de pare-feu entrants et sortants pour les hôtes ESXi », page 69 pour obtenir une liste de ports.

Connexion à la console de machine virtuelle via un pare-feu

Certains ports doivent être ouverts pour la communication utilisateur et administrateur avec la console de machine virtuelle. Les ports nécessitant d'être ouverts varient selon le type de console de machine virtuelle et si vous vous connectez via vCenter Server avec vSphere Web Client ou directement à l'hôte ESXi depuis VMware Host Client.

Connexion à une console de machine virtuelle basée sur une interface de navigation au moyen vSphere Web Client

Lorsque vous vous connectez avec vSphere Web Client, vous vous connectez toujours au système vCenter Server qui gère l'hôte ESXi et accédez à la console de machine virtuelle depuis là.

Si vous utilisez vSphere Web Client et que vous vous connectez à une console de machine virtuelle basée sur une interface de navigation, l'accès suivant doit être possible :

- Le pare-feu doit autoriser vSphere Web Client à accéder à vCenter Server par le port 9443.
- Le pare-feu doit autoriser vCenter Server à accéder à ESXi par le port 902.

Connexion à une console de machine virtuelle autonome au moyen vSphere Web Client

Si vous utilisez vSphere Web Client et que vous vous connectez à une console de machine virtuelle autonome, l'accès suivant doit être possible :

- Le pare-feu doit autoriser vSphere Web Client à accéder à vCenter Server par le port 9443.
- Le pare-feu doit autoriser la console de machine virtuelle à accéder à vCenter Server par le port 9443 et à l'hôte ESXi par le port 902.

Connexion aux hôtes ESXi directement avec VMware Host Client

Vous pouvez utiliser la console de machine virtuelle VMware Host Client si vous vous connectez directement à un hôte ESXi.

Remarque N'utilisez pas VMware Host Client pour vous connecter directement aux hôtes gérés par un système vCenter Server. Si vous apportez des modifications à ces hôtes depuis VMware Host Client, votre environnement devient instable.

Le pare-feu doit autoriser l'accès à l'hôte ESXi sur les ports 443 et 902

VMware Host Client utilise le port 902 pour fournir une connexion aux activités MKS du système d'exploitation invité sur les machines virtuelles. C'est par ce port que les utilisateurs interagissent avec les systèmes d'exploitation et les applications invités de la machine virtuelle. VMware ne prend pas en charge la configuration d'un port différent pour cette fonction.

Sécuriser le commutateur physique

Sécurisez le commutateur physique sur chaque hôte ESXi pour empêcher les pirates d'obtenir accès à l'hôte et à ses machines virtuelles.

Pour garantir la meilleure protection de vos hôtes, assurez-vous que la configuration des ports du commutateur physique désactive le protocole STP (Spanning Tree Protocol) et que l'option de non-négociation est configurée pour les liaisons de jonction entre les commutateurs physiques externes et les commutateurs virtuels en mode VST (Virtual Switch Tagging).

Procédure

1 Connectez-vous au commutateur physique et assurez-vous que le protocole Spanning Tree est désactivé ou que PortFast est configuré pour tous les ports de commutateur physique qui sont connectés aux hôtes ESXi.

2 Pour des machines virtuelles qui effectuent un pontage ou un routage, vérifiez périodiquement que la configuration du premier port de commutateur physique en amont désactive BPDU Guard et PortFast et active le protocole Spanning Tree.

   Dans vSphere 5.1 et versions ultérieures, pour protéger le commutateur physique des attaques de déni de service (DoS), vous pouvez activer le filtrage BPDU invité sur les hôtes ESXi.

3 Connectez-vous au commutateur physique et assurez-vous que le protocole DTP (Dynamic Trunking Protocol) n'est pas activé sur les ports du commutateur physique qui sont connectés aux hôtes ESXi.

4 Vérifiez régulièrement les ports du commutateur physique pour vous assurer qu'ils sont correctement configurés comme ports de jonction s'ils sont connectés à des ports de jonction VLAN d'un commutateur virtuel.

Sécurisation des ports du commutateur standard à l'aide de stratégies de sécurité

Tout comme pour les adaptateurs réseau physiques, un adaptateur réseau de machine virtuelle peut envoyer des trames qui semblent provenir d'une autre machine ou emprunter l'identité d'une autre machine afin de pouvoir recevoir des trames réseau destinées à cette machine. Par conséquent, tout comme les adaptateurs réseau physiques, un adaptateur réseau de machine virtuelle peut être configuré afin de recevoir des trames destinées à d'autres machines. Ces deux scénarios représentent un risque pour la sécurité.

Lorsque vous créez un commutateur standard pour votre réseau, vous ajoutez des groupes de ports dans vSphere Web Client pour imposer aux machines virtuelles et aux adaptateurs VMkernel une stratégie concernant le trafic système lié au commutateur.

Dans le cadre de l'ajout d'un groupe de ports VMkernel ou d'un groupe de ports de machine virtuelle à un commutateur standard, ESXi configure une stratégie de sécurité pour les ports du groupe. Vous pouvez utiliser ce profil de sécurité pour garantir que l'hôte empêche les systèmes d'exploitation invités de ses machines virtuelles d'emprunter l'identité d'autres machines sur le réseau. Cette fonction de sécurité est implémentée afin que le système d'exploitation invité responsable de l'emprunt d'identité ne détecte pas que l'emprunt d'identité a été empêché.

La stratégie de sécurité détermine le niveau d'intensité avec lequel vous appliquez la protection contre l'emprunt d'identité et les attaques d'interception sur les machines virtuelles. Pour utiliser correctement les paramètres du profil de sécurité, vous devez comprendre comment les adaptateurs réseau de machines virtuelles contrôlent les transmissions et la manière dont les attaques sont contrées à ce niveau. Consultez la section Stratégies de sécurité dans *Mise en réseau vSphere*.

.

Sécuriser les commutateurs standard vSphere

Vous pouvez sécuriser le trafic de commutation standard contre les attaques de couche 2 en limitant certains modes d'adresses MAC à l'aide des paramètres de sécurité des commutateurs.

Chaque adaptateur réseau de la machine virtuelle dispose d'une adresse MAC initiale et d'une adresse MAC effective.

Adresse MAC initiale L'adresse MAC initiale est attribuée lors de la création de l'adaptateur. Bien que l'adresse MAC initiale puisse être reconfigurée à partir de l'extérieur du système d'exploitation invité, elle ne peut pas être modifiée par le système d'exploitation invité.

Adresse MAC effective Chaque adaptateur dispose d'une adresse MAC effective qui filtre le trafic réseau entrant avec une adresse MAC de destination différente de l'adresse MAC effective. Le système d'exploitation invité est responsable de la définition de l'adresse MAC effective et fait généralement correspondre l'adresse MAC effective à l'adresse MAC initiale.

Lors de la création de l'adaptateur réseau d'une machine virtuelle, l'adresse MAC effective et l'adresse MAC initiale sont identiques. Le système d'exploitation invité peut à tout moment remplacer l'adresse MAC effective par une autre valeur. Si un système d'exploitation modifie l'adresse MAC effective, son adaptateur réseau reçoit le trafic réseau destiné à la nouvelle adresse MAC.

Lors de l'envoi de paquets via un adaptateur réseau, le système d'exploitation invité place généralement sa propre adresse MAC effective de l'adaptateur dans la zone de l'adresse MAC source des trames Ethernet. Il place l'adresse MAC de l'adaptateur réseau récepteur dans la zone d'adresse MAC de destination. L'adaptateur récepteur accepte les paquets uniquement si l'adresse MAC de destination du paquet correspond à sa propre adresse MAC effective.

Un système d'exploitation peut envoyer des trames avec une adresse MAC source usurpée. Cela signifie qu'un système d'exploitation peut bloquer les attaques nuisibles sur les périphériques dans un réseau en empruntant l'identité d'un adaptateur réseau que le réseau récepteur autorise.

Protégez le trafic virtuel contre l'emprunt d'identité et les attaques de couche 2 d'interception en configurant une stratégie de sécurité sur les groupes de ports ou les ports.

La stratégie de sécurité sur les groupes de ports distribués et les ports inclut les options suivantes :

- Mode promiscuité (reportez-vous à « Fonctionnement en mode promiscuité », page 170)
- Modifications d'adresse MAC (reportez-vous à « Modifications d'adresse MAC », page 169)
- Transmissions forgées (reportez-vous à « Transmissions forgées », page 170)

Vous pouvez afficher et modifier les paramètres par défaut en sélectionnant le commutateur virtuel associé à l'hôte dans vSphere Web Client. Consultez la documentation de *Mise en réseau vSphere*.

Modifications d'adresse MAC

La règle de sécurité d'un commutateur virtuel inclut une option **Modifications d'adresse MAC**. Cette option affecte le trafic qu'une machine virtuelle reçoit.

Lorsque l'option **Modifications d'adresse Mac** est définie sur **Accepter**, ESXi accepte les demandes de modification de l'adresse MAC effective en une adresse différente de l'adresse MAC initiale.

Lorsque l'option **Modifications d'adresse Mac** est définie sur **Rejeter**, ESXi n'honore pas les demandes de modification de l'adresse MAC effective en une adresse différente de l'adresse MAC initiale. Ce paramètre protège l'hôte contre l'emprunt d'identité MAC. Le port que l'adaptateur de machine virtuelle a utilisé pour envoyer la demande est désactivé et l'adaptateur de machine virtuelle ne reçoit plus de trames jusqu'à ce que l'adresse MAC effective corresponde à l'adresse MAC initiale. Le système d'exploitation invité ne détecte pas que la demande de modification d'adresse MAC n'a pas été honorée.

Remarque L'initiateur iSCSI repose sur la capacité à obtenir les modifications d'adresse MAC de certains types de stockage. Si vous utilisez iSCSI ESXi avec un stockage iSCSI, définissez l'option **Modifications d'adresse MAC** sur **Accepter**.

Dans certaines situations, vous pouvez avoir un besoin légitime d'attribuer la même adresse MAC à plusieurs adaptateurs, par exemple, si vous utilisez l'équilibrage de la charge réseau Microsoft en mode monodiffusion. Lorsque l'équilibrage de la charge réseau Microsoft est utilisé en mode multidiffusion standard, les adaptateurs ne partagent pas les adresses MAC.

Transmissions forgées

L'option **Transmissions forgées** affecte le trafic transmis à partir d'une machine virtuelle.

Lorsque l'option **Transmissions forgées** est définie sur **Accepter**, ESXi ne compare les adresses MAC source et effective.

Pour se protéger d'un emprunt d'identité MAC, vous pouvez définir l'option **Transmissions forgées** sur **Rejeter**. Dans ce cas, l'hôte compare l'adresse MAC source que transmet le système d'exploitation invité avec l'adresse MAC effective de son adaptateur de machine virtuelle pour déterminer si elles correspondent. Si elles ne correspondent pas, l'hôte ESXi abandonne le paquet.

Le système d'exploitation invité ne détecte pas que son adaptateur de machine virtuelle ne peut pas envoyer de paquets à l'aide de l'adresse MAC usurpée. L'hôte ESXi intercepte les paquets avec des adresses usurpées avant leur livraison, et le système d'exploitation invité peut supposer que les paquets sont rejetés.

Fonctionnement en mode promiscuité

Le mode promiscuité élimine tout filtrage de réception que l'adaptateur de machine virtuelle peut effectuer afin que le système d'exploitation invité reçoive tout le trafic observé sur le réseau. Par défaut, l'adaptateur de machine virtuelle ne peut pas fonctionner en mode promiscuité.

Bien que le mode promiscuité puisse être utile pour le suivi de l'activité réseau, c'est un mode de fonctionnement non sécurisé, car les adaptateurs en mode promiscuité ont accès aux paquets, même si certains de ces paquets sont reçus uniquement par un adaptateur réseau spécifique. Cela signifie qu'un administrateur ou un utilisateur racine dans une machine virtuelle peut potentiellement voir le trafic destiné à d'autres systèmes d'exploitation hôtes ou invités.

Remarque Dans certaines situations, vous pouvez avoir une raison légitime de configurer un commutateur virtuel standard ou distribué pour fonctionner en mode promiscuité ; par exemple, si vous exécutez un logiciel de détection des intrusions réseau ou un renifleur de paquets.

Sécuriser les commutateurs distribués vSphere et les groupes de ports distribués

Les administrateurs disposent de plusieurs options pour sécuriser un vSphere Distributed Switch dans leur environnement vSphere.

Procédure

1 Pour les groupes de ports distribués avec une liaison statique, vérifiez que la fonction Extension automatique est désactivée.

Extension automatique est activée par défaut dans vSphere 5.1 et versions ultérieures.

Pour désactiver Extension automatique, configurez la propriété `autoExpand` sous le groupe de ports distribués avec vSphere Web Services SDK ou avec une interface de ligne de commande. Reportez-vous à la documentation *vSphere Web Services SDK*.

2 Assurez-vous que tous les ID VLAN privés de tout vSphere Distributed Switch sont entièrement documentés.

3 Si vous utilisez le balisage VLAN sur un dvPortgroup, les ID de VLAN doivent correspondre aux ID des commutateurs VLAN externes en amont. Si les ID de VLAN ne sont pas entièrement suivis, une réutilisation erronée d'ID peut permettre l'établissement de trafic entre des machines physiques et virtuelles non appropriées. De la même manière, si des ID de VLAN sont incorrects ou manquants, le trafic risque de ne pas être transmis entre les machines physiques et virtuelles.

4 Vérifiez l'absence de ports inutilisés sur un groupe de ports virtuels associé à un vSphere Distributed Switch.

5 Attribuez un libellé à chaque vSphere Distributed Switch.

Les vSphere Distributed Switches associés à un hôte ESXi nécessitent un champ pour le nom du commutateur. Ce libellé sert de descripteur fonctionnel du commutateur, de même qu'un nom d'hôte associé à un commutateur physique. Le libellé du vSphere Distributed Switch indique la fonction ou le sous-réseau IP du commutateur. Par exemple, vous pouvez attribuer le libellé « interne » au commutateur pour indiquer qu'il est destiné uniquement à la mise en réseau interne d'un commutateur virtuel privé de machine virtuelle, sans liaison avec des adapteurs réseau physiques.

6 Désactivez le contrôle de santé du réseau pour vos vSphere Distributed Switches si vous ne l'utilisez pas activement.

Le contrôle de santé du réseau est désactivé par défaut. Une fois qu'il est activé, les paquets de contrôle de santé contiennent des informations sur l'hôte, le commutateur et le port, susceptibles d'être utilisées par un pirate. N'utilisez le contrôle de santé du réseau que pour le dépannage et désactivez-le lorsque le dépannage est terminé.

7 Protégez le trafic virtuel contre l'emprunt d'identité et les attaques de couche 2 d'interception en configurant une stratégie de sécurité sur les groupes de ports ou les ports.

La stratégie de sécurité sur les groupes de ports distribués et les ports inclut les options suivantes :

- Mode promiscuité (reportez-vous à « Fonctionnement en mode promiscuité », page 170)
- Modifications d'adresse MAC (reportez-vous à « Modifications d'adresse MAC », page 169)
- Transmissions forgées (reportez-vous à « Transmissions forgées », page 170)

Pour consulter les paramètres actuels et les modifier, sélectionnez **Gérer des groupes de ports distribués** dans le menu contextuel (bouton droit de la souris) du Distributed Switch, puis sélectionnez **Sécurité** dans l'assistant. Consultez la documentation de *Mise en réseau vSphere*.

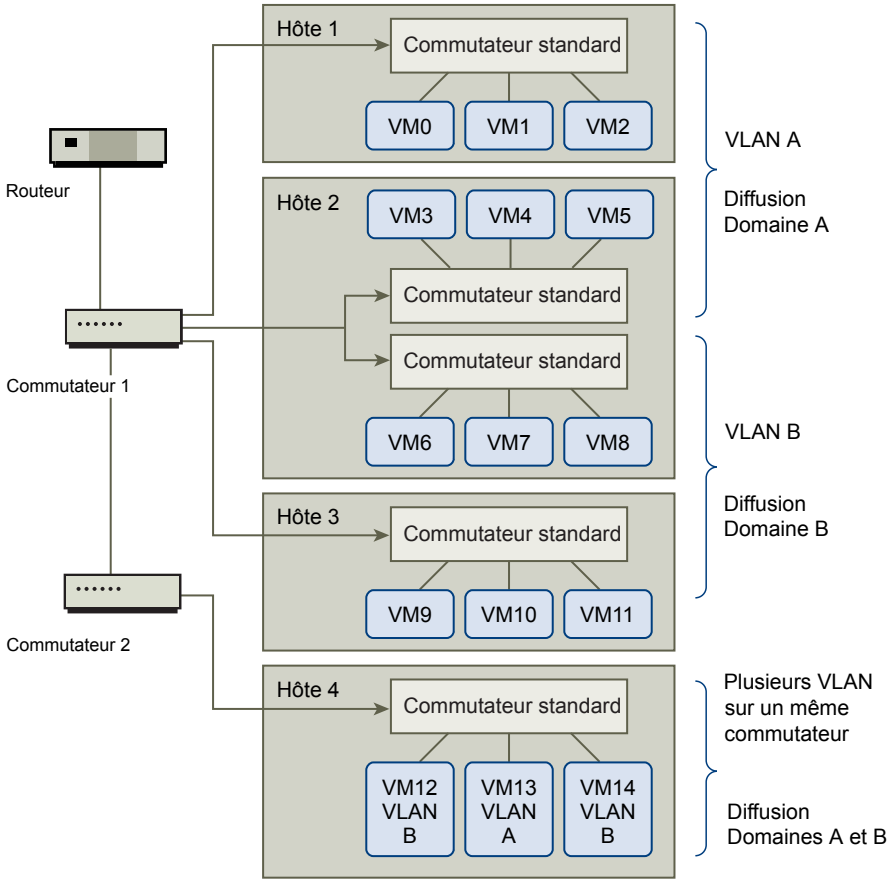
Sécurisation des machines virtuelles avec des VLAN

Le réseau peut être l'une des parties les plus vulnérables d'un système. Votre réseau de machines virtuelles nécessite autant de protection que votre réseau physique. L'utilisation des VLAN peut permettre d'améliorer la sécurité réseau dans votre environnement.

Les VLAN sont un schéma de réseau standard IEEE avec des méthodes de balisage spécifiques qui permettent le routage des paquets uniquement vers les ports faisant partie du VLAN. S'ils sont configurés correctement, les VLAN fournissent un moyen fiable pour protéger un ensemble de machines virtuelles des intrusions accidentelles et nuisibles.

Les VLAN vous permettent de segmenter un réseau physique afin que deux machines du réseau ne puissent pas transmettre et recevoir des paquets à moins de faire partie du même VLAN. Par exemple, les enregistrements de comptabilité et les transactions font partie des informations internes les plus sensibles d'une entreprise. Dans une entreprise dont les employés des ventes, des expéditions et de la comptabilité utilisent tous des machines virtuelles sur le même réseau physique, vous pouvez protéger les machines virtuelles du service de comptabilité en configurant des VLAN.

Figure 8-1. Exemple de disposition de VLAN



Dans cette configuration, tous les employés du service de comptabilité utilisent des machines virtuelles dans un VLAN A et les employés des ventes utilisent des machines virtuelles dans VLAN B.

Le routeur transmet les paquets contenant les données de comptabilité aux commutateurs. Ces paquets sont balisés pour une distribution sur le VLAN A uniquement. Par conséquent, les données sont confinées à une diffusion dans le domaine A et ne peuvent pas être acheminées pour une diffusion dans le domaine B à moins que le routeur ne soit configuré pour le faire.

Cette configuration de VLAN empêche les forces de vente d'intercepter les paquets destinés au service de comptabilité. Elle empêche également le service de comptabilité de recevoir des paquets destinés au groupes de ventes. Les machines virtuelles prises en charge par un seul commutateur virtuel peuvent se trouver sur des VLAN différents.

Considérations relatives à la sécurité pour les VLAN

La manière dont vous configurez les VLAN pour sécuriser des parties du réseau dépend de facteurs tels que le système d'exploitation invité et la façon dont votre équipement réseau est configuré.

ESXi dispose d'une implémentation VLAN complète conforme IEEE 802.1q. VMware ne peut pas faire de recommandations spécifiques sur la manière de configurer des VLAN, mais il existe des facteurs à prendre en compte lors de l'utilisation d'un déploiement VLAN dans le cadre de votre stratégie d'application de la sécurité.

Sécuriser les VLAN

Les administrateurs disposent de plusieurs options permettant de sécuriser les réseaux VLAN dans leur environnement vSphere.

Procédure

1 Assurez-vous que les groupes de ports ne sont pas configurés pour des valeurs VLAN réservées par les commutateurs physiques en amont

   Ne définissez pas de valeurs ID VLAN réservées au commutateur physique.

2 Assurez-vous que les groupes de ports ne sont pas configurés sur VLAN 4095, sauf si vous utilisez le balisage d'invité virtuel (VGT).

   Il existe trois types de balisage VLAN dans vSphere :

   - Balisage de commutateur externe (EST)
   - Balisage de commutateur virtuel (VST) - Le commutateur virtuel marque avec l'ID de VLAN le trafic qui entre dans les machines virtuelles attachées et supprime la balise VLAN du trafic qui les quitte. Pour configurer le mode VST, attribuez un ID VLAN compris entre 1 et 4095.
   - Balisage d'invité virtuel (VGT) - Les machines virtuelles gèrent le trafic VLAN. Pour activer le mode VGT, définissez l'ID VLAN sur 4095. Sur un commutateur distribué, vous pouvez également autoriser le trafic d'une machine virtuelle en fonction de son réseau VLAN à l'aide de l'option **Jonction VLAN**.

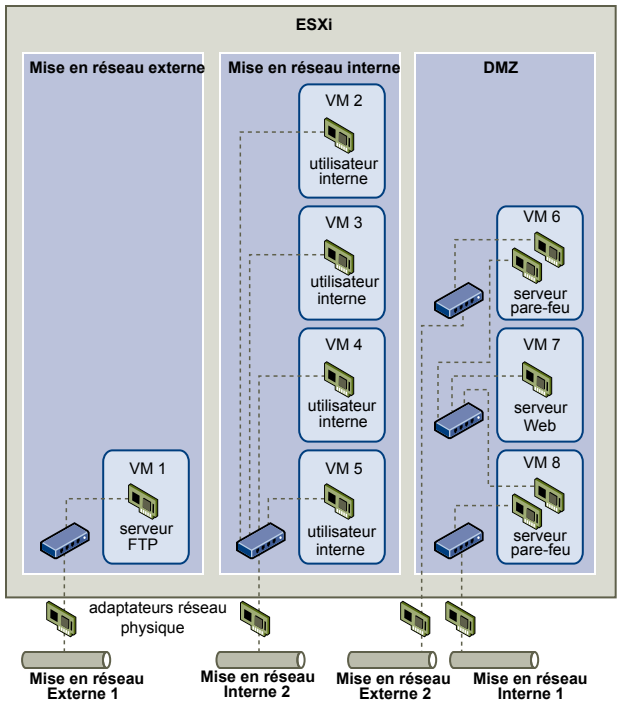
   Sur un commutateur standard, vous pouvez configurer le mode de mise en réseau VLAN au niveau du commutateur ou du groupe de ports, et sur un commutateur distribué au niveau du groupe de ports distribués ou du port.

3 Assurez-vous que tous les réseaux VLAN de chaque commutateur virtuel sont pleinement documentés et que chaque commutateur virtuel dispose de tous les VLAN requis et des VLAN seulement nécessaires.

Création de plusieurs réseaux sur un hôte ESXi

Le système ESXi a été conçu pour vous permettre de connecter certains groupes de machines virtuelles au réseau interne, ainsi que d'autres groupes au réseau externe, et enfin d'autres groupes aux deux réseaux, le tout sur le même hôte. Cette capacité est une extension de l'isolation de machines virtuelles ; elle est associée à une optimisation de la planification d'utilisation des fonctions de réseau virtuel.

Figure 8-2. Réseaux externes, réseaux internes et DMZ configurée sur un hôte ESXi unique



Dans la figure, l'administrateur système a configuré un hôte dans trois zones différentes de machine virtuelle : sur le serveur FTP, dans les machines virtuelles et dans la zone démilitarisée (DMZ). Chacune de ces zones a une fonction spécifique.

Serveur FTP

La machine virtuelle 1 est configurée avec logiciel FTP et sert de zone de rétention des données envoyées de et vers des ressources extérieures (formulaires et collatéraux localisés par un fournisseur, par exemple).

Cette machine virtuelle est associée à un réseau externe uniquement. Elle possède son propre commutateur virtuel et sa propre carte de réseau physique, qui lui permettent de se connecter au réseau externe 1. Ce réseau est réservé aux serveurs utilisés par l'entreprise pour la réception de données issues de sources externes. Par exemple, l'entreprise peut utiliser le réseau externe 1 pour recevoir un trafic FTP en provenance de leurs fournisseurs, et pour permettre à ces derniers d'accéder aux données stockées sur des serveurs externes via FTP. Outre la machine virtuelle 1, le réseau externe 1 sert les serveurs FTP configurés sur différents hôtes ESXi du site.

La machine virtuelle 1 ne partage pas de commutateur virtuel ou de carte de réseau physique avec les machines virtuelles de l'hôte ; par conséquent, les autres machines virtuelles ne peuvent pas acheminer de paquets de et vers le réseau de la machine virtuelle 1. Cette restriction évite les intrusions, qui nécessitent l'envoi de trafic réseau à la victime. Plus important encore : un pirate ne peut pas exploiter la vulnérabilité naturelle du protocole FTP pour accéder aux autres machines virtuelles de l'hôte.

Machines virtuelles internes

Les machines virtuelles 2 à 5 sont réservées à une utilisation interne. Ces machines virtuelles traitent et stockent les données confidentielles des entreprises (dossiers médicaux, jugements ou enquêtes sur la fraude, par exemple). Les administrateurs systèmes doivent donc leur associer un niveau maximal de protection.

Elles se connectent au réseau interne 2 via leur propre commutateur virtuel et leur propre carte réseau. Le réseau interne 2 est réservé à une utilisation interne par le personnel approprié (responsables de dossiers d'indemnisation ou juristes internes, par exemple).

Les machines virtuelles 2 à 5 peuvent communiquer entre elles via le commutateur virtuel ; elles peuvent aussi communiquer avec les machines virtuelles du réseau interne 2 via la carte réseau physique. En revanche, elles ne peuvent pas communiquer avec des machines externes. Comme pour le serveur FTP, ces machines virtuelles ne peuvent pas acheminer des paquets vers ou les recevoir depuis les réseaux des autres machines virtuelles. De la même façon, les autres machines virtuelles de l'hôte ne peuvent pas acheminer des paquets vers ou les recevoir depuis les machines virtuelles 2 à 5.

DMZ

Les machines virtuelles 6 à 8 sont configurées en tant que zone démilitarisée (DMZ) ; le groupe marketing les utilise pour publier le site Web externe de l'entreprise.

Ce groupe de machines virtuelles est associé au réseau externe 2 et au réseau interne 1. L'entreprise utilise le réseau externe 2 pour les serveurs Web qui hébergent le site Web de l'entreprise et d'autres outils Web destinés à des utilisateurs externes. Le réseau interne 1 est utilisé par le service marketing pour publier le contenu du site Web de l'entreprise, pour effectuer des téléchargements et pour gérer des services tels que des forums utilisateur.

Puisque ces réseaux sont séparés du réseau externe 1 et du réseau interne 2, et que les machines virtuelles n'ont pas de point de contact partagé (commutateurs ou adaptateurs), il n'y a aucun risque d'attaque de ou vers le serveur FTP ou le groupe de machines virtuelles internes.

Grâce à l'isolation des machines virtuelles, à la bonne configuration des commutateurs virtuels et à la séparation des réseaux, l'administrateur système peut inclure les trois zones de machines virtuelles sur le même hôte ESXi et être rassuré quant à l'absence de violations de données ou de ressources.

L'entreprise met en œuvre l'isolation au sein des groupes de machines virtuelles via l'utilisation de plusieurs réseaux internes et externes, et via la séparation des commutateurs virtuels et des adaptateurs réseau physiques de chaque groupe.

Aucun des commutateurs virtuels ne fait le lien entre les différentes zones de machines virtuelles ; l'administrateur système peut donc éliminer tout risque de fuite de paquets d'une zone à l'autre. Au niveau de sa conception même, un commutateur virtuel ne peut pas transmettre directement des paquets vers un autre commutateur virtuel Pour acheminer des paquets d'un commutateur virtuel vers un autre, les conditions suivantes doivent être réunies :

- Les commutateurs virtuels doivent être connectés au même réseau local physique.

- Les commutateurs virtuels doivent se connecter à une machine virtuelle commune, qui peut être utilisée pour la transmission de paquets.

Or, aucune de ces situations ne se vérifie dans l'exemple de configuration. Si les administrateurs système souhaitent vérifier l'absence de chemin commun de commutateur virtuel, ils peuvent rechercher les éventuels points de contact partagés en examinant la disposition des commutateurs réseau dans vSphere Web Client.

Pour protéger les ressources des machines virtuelles, l'administrateur système diminue le risque d'attaque DoS et DDoS en configurant une réservation de ressources, ainsi qu'une limite applicable à chaque machine virtuelle. Il renforce la protection de l'hôte ESXi et des machines virtuelles en installant des pare-feu sur la partie frontale et la partie principale de la zone démilitarisée (DMZ), en vérifiant que l'hôte est protégé par un pare-feu physique et en configurant les ressources de stockage réseau de telle sorte qu'elles bénéficient toutes de leur propre commutateur virtuel.

Sécurité du protocole Internet

La sécurité du protocole Internet (IPsec) sécurise les communications IP provenant de et arrivant sur l'hôte. Les hôtes ESXi prennent en charge IPsec utilisant IPv6.

Lorsque vous configurez IPsec sur un hôte, vous activez l'authentification et le chiffrement des paquets entrants et sortants. Le moment et la manière dont le trafic IP est chiffré dépendent de la façon dont vous avez configuré les associations de sécurité et les règles de sécurité du système.

Une association de sécurité détermine comment le système chiffre le trafic. Lorsque vous créez une association de sécurité, vous indiquez la source et la destination, les paramètres de chiffrement et le nom de l'association de sécurité.

Une stratégie de sécurité détermine le moment auquel le système doit chiffrer le trafic. La stratégie de sécurité comprend les informations de source et de destination, le protocole et la direction du trafic à chiffrer, le mode (transport ou tunnel) et l'association de sécurité à utiliser.

Liste des associations de sécurité disponibles

ESXi peut fournir une liste de toutes les associations de sécurité disponibles pour l'utilisation par les règles de sécurité. Cette liste inclut les associations de sécurité créées par l'utilisateur et les associations de sécurité que VMkernel a installées à l'aide d'Internet Key Exchange.

Vous pouvez obtenir une liste des associations de sécurité disponibles à l'aide de la commande vSphere CLI `esxcli`.

Procédure

- Dans l'invite de commande, entrez la commande **`esxcli network ip ipsec sa list`**.

ESXi affiche une liste de toutes les associations de sécurité disponibles.

Ajouter une association de sécurité IPsec

Ajoutez une association de sécurité pour définir des paramètres de chiffrement pour le trafic IP associé.

Vous pouvez ajouter une association de sécurité avec la commande vSphere CLI `esxcli`.

Procédure

- Dans l'invite de commande, saisissez la commande **`esxcli network ip ipsec sa add`** avec une ou plusieurs des options suivantes.

Option	Description
`--sa-source=` ***source address***	Requis. Spécifiez l'adresse source.
`--sa-destination=` ***destination address***	Requis. Spécifiez l'adresse de destination.
`--sa-mode=` ***mode***	Requis. Spécifiez le mode, soit `transport` ou `tunnel`.
`--sa-spi=` ***security parameter index***	Requis. Spécifiez l'index des paramètres de sécurité. Celui-ci identifie l'association de sécurité à l'hôte. Ce doit être un hexadécimal avec un préfixe 0x. Chaque association de sécurité que vous créez doit disposer d'une combinaison unique de protocole et d'index de paramètres de sécurité.
`--encryption-algorithm=` ***encryption algorithm***	Requis. Spécifiez l'algorithme de chiffrement à l'aide d'un des paramètres suivants. ■ `3des-cbc` ■ `aes128-cbc` ■ `null` (n'assure aucun chiffrage)
`--encryption-key=` ***encryption key***	Requise lorsque vous spécifiez un algorithme de chiffrement. Spécifiez la clé de chiffrement. Vous pouvez entrer des clés en tant que texte ASCII ou en tant qu'hexadécimal avec un préfixe 0x.
`--integrity-algorithm=` ***authentication algorithm***	Requis. Spécifiez l'algorithme d'authentification, soit `hmac-sha1` ou `hmac-sha2-256`.
`--integrity-key=` ***authentication key***	Requis. Spécifiez la clé d'authentification. Vous pouvez entrer des clés en tant que texte ASCII ou en tant qu'hexadécimal avec un préfixe 0x.
`--sa-name=`***name***	Requis. Indiquez un nom pour l'association de sécurité.

Exemple : Commande de nouvelle association de sécurité

L'exemple suivant contient des sauts de ligne supplémentaires pour des raisons de lisibilité.

```
esxcli network ip ipsec sa add
--sa-source 3ffe:501:ffff:0::a
--sa-destination 3ffe:501:ffff:0001:0000:0000:0000:0001
--sa-mode transport
--sa-spi 0x1000
--encryption-algorithm 3des-cbc
--encryption-key 0x69707636726561647 96c6f676f33646573636236f757432
--integrity-algorithm hmac-sha1
--integrity-key 0x6970763672656164796c6f67736861316f757432
--sa-name sa1
```

Supprimer une association de sécurité IPsec

Vous pouvez supprimer une association de sécurité avec la commande vSphere CLI ESXCLI.

Prérequis

Vérifiez que l'association de sécurité que vous souhaitez employer n'est pas actuellement utilisée. Si vous essayez de supprimer une association de sécurité en cours d'utilisation, l'opération de suppression échoue.

Procédure

- À la suite de l'invite de commande, entrez la commande **`esxcli network ip ipsec sa remove --sa-name`*****security_association_name***.

Répertorier les stratégies de sécurité IPsec disponibles

Vous pouvez répertorier les stratégies de sécurité disponibles à l'aide de la commande vSphere CLI ESXCLI.

Procédure

- À la suite de l'invite de commande, entrez la commande **`esxcli network ip ipsec sp list`**.

L'hôte affiche une liste de toutes les règles de sécurité disponibles.

Créer une stratégie de sécurité IPSec

Créez une règle de sécurité pour déterminer le moment auquel utiliser les paramètres d'authentification et de chiffrement définis dans une association de sécurité. Vous pouvez ajouter une stratégie de sécurité à l'aide de la commande vSphere CLI ESXCLI.

Prérequis

Avant de créer une règle de sécurité, ajoutez une association de sécurité comportant les paramètres d'authentification et de chiffrement appropriés décrits dans « Ajouter une association de sécurité IPsec », page 176.

Procédure

- Dans l'invite de commande, saisissez la commande **`esxcli network ip ipsec sp add`** avec une ou plusieurs des options suivantes.

Option	Description
`--sp-source=` ***source address***	Requis. Spécifiez l'adresse IP source et la longueur du préfixe.
`--sp-destination=` ***destination address***	Requis. Spécifiez l'adresse de destination et la longueur du préfixe.
`--source-port=` ***port***	Requis. Spécifiez le port source. Le port source doit être un nombre compris entre 0 et 65 535.
`--destination-port=` ***port***	Requis. Spécifiez le port de destination. Le port source doit être un nombre compris entre 0 et 65 535.
`--upper-layer-protocol=` ***protocol***	Spécifiez le protocole de couche supérieure à l'aide d'un des paramètres suivants. ■ `tcp` ■ `udp` ■ `icmp6` ■ `toutes`
`--flow-direction=` ***direction***	Spécifiez la direction dans laquelle vous souhaitez surveiller le trafic à l'aide de `in` ou `out`.
`--action=` ***action***	Définissez l'action à prendre lorsque le trafic avec les paramètres spécifiés est rencontré à l'aide des paramètres suivants. ■ `none` : Ne faites rien ■ `discard` : Ne permettez pas l'entrée ou la sortie de données. ■ `ipsec` : Utilisez les informations d'authentification et de chiffrement fournies dans l'association de sécurité pour déterminer si les données proviennent d'une source de confiance.
`--sp-mode=` ***mode***	Spécifiez le mode, soit `tunnel` ou `transport`.
**`--sa-name=`*security association name*	Requis. Indiquez le nom de l'association de sécurité pour la règle de sécurité à utiliser.
**`--sp-name=`*name*	Requis. Indiquez un nom pour la règle de sécurité.

Exemple : Commande de nouvelle règle de sécurité

L'exemple suivant contient des sauts de ligne supplémentaires pour des raisons de lisibilité.

```
esxcli network ip ipsec add
--sp-source=2001:db8:1::/64
--sp-destination=2002:db8:1::/64
--source-port=23
--destination-port=25
--upper-layer-protocol=tcp
--flow-direction=out
--action=ipsec
--sp-mode=transport
--sa-name=sa1
--sp-name=sp1
```

Supprimer une stratégie de sécurité IPsec

Vous pouvez supprimer une stratégie de sécurité de l'hôte ESXi à l'aide de la commande vSphere CLI ESXCLI.

Prérequis

Vérifiez que la stratégie de sécurité que vous souhaitez utiliser n'est pas actuellement utilisée. Si vous essayez de supprimer une règle de sécurité en cours d'utilisation, l'opération de suppression échoue.

Procédure

- Dans l'invite de commande, entrez la commande **`esxcli network ip ipsec sp remove --sa-name`** ***`security policy name`***.

  Pour supprimer toutes les règles de sécurité, entrez la commande **`esxcli network ip ipsec sp remove --remove-all`**.

Garantir une configuration SNMP appropriée

Si SNMP n'est pas configuré correctement, les informations de surveillance peuvent être envoyées à un hôte malveillant. L'hôte malveillant peut ensuite utiliser ces informations pour planifier une attaque.

SNMP doit être configuré sur chaque hôte ESXi. Vous pouvez utiliser vCLI, PowerCLI ou vSphere Web Services SDK pour la configuration.

Procédure

1. Exécutez `esxcli system snmp get` pour déterminer si SNMP est actuellement utilisé.
2. Si votre système ne requiert pas SNMP, assurez-vous qu'il est en cours d'exécution en exécutant la commande `esxcli system snmp set --enable true`.
3. Si votre système utilise SNMP, consultez la publication *Surveillance et performances* pour obtenir des informations sur la configuration de SNMP 3.

Meilleures pratiques en matière de sécurité de la mise en réseau vSphere

L'observation des recommandations en matière de sécurité contribue à garantir l'intégrité de votre déploiement vSphere.

Recommandations générales de sécurité pour la mise en réseau

En matière de sécurisation de votre environnement réseau, la première étape consiste à respecter les recommandations de sécurité générales s'appliquant aux réseaux. Vous pouvez ensuite vous concentrer sur des points spéciaux, comme la sécurisation du réseau à l'aide de pare-feu ou du protocole IPsec.

- Si Spanning Tree est activé, assurez-vous que les ports du commutateur physique sont configurés avec Portfast. Étant donné que les commutateurs virtuels VMware ne prennent pas en charge le STP, Portfast doit être configuré sur les ports de commutateur physique connectés à un hôte ESXi, afin d'éviter les boucles au sein du réseau de commutateurs physiques. Si le protocole Portfast n'est pas configuré, des problèmes de performance et de connectivité sont à craindre.
- Assurez-vous que le trafic NetFlow d'un Distributed Virtual Switch est envoyé uniquement aux adresses IP de collecteurs autorisés. Les exportations Netflow ne sont pas chiffrées et peuvent contenir des informations sur le réseau virtuel. Ces informations augmentent les risques d'attaque de type « intermédiaire ». Si une exportation Netflow est nécessaire, assurez-vous que toutes les adresses IP Netflow cibles sont correctes.
- Assurez-vous que seuls les administrateurs autorisés ont accès aux composants de mise en réseau en utilisant des contrôles d'accès basés sur rôles. Par exemple, les administrateurs de machines virtuelles ne devraient pouvoir accéder qu'aux groupes de ports dans lesquels leurs machines virtuelles résident. Donnez aux administrateurs réseau des autorisations pour tous les composants du réseau virtuel, mais pas d'accès aux machines virtuelles. Le fait de limiter l'accès réduit le risque d'erreur de configuration, qu'elle soit accidentelle ou délibérée, et renforce les concepts essentiels de sécurité que sont la séparation des devoirs et le moindre privilège.
- Assurez-vous que les groupes de ports ne sont pas configurés sur la valeur du VLAN natif. Les commutateurs physiques utilisent VLAN 1 comme VLAN natif. Les trames sur un VLAN natif ne sont pas balisées avec un 1. ESXi n'a pas de VLAN natif. Les trames pour lesquelles le VLAN est spécifié dans le groupe de ports comportent une balise, mais les trames pour lesquelles le VLAN n'est pas spécifié dans le groupe de ports ne sont pas balisées. Ceci peut créer un problème, car les machines virtuelles balisées avec un 1 appartiendront au VLAN natif du commutateur physique.

  Par exemple, les trames sur le VLAN 1 d'un commutateur physique Cisco ne sont pas balisées car VLAN1 est le VLAN natif sur ce commutateur physique. Cependant, les trames de l'hôte ESXi qui sont spécifiées en tant que VLAN 1 sont balisées avec un 1. Par conséquent, le trafic de l'hôte ESXi destiné au VLAN natif n'est pas routé correctement, car il est balisé avec un 1 au lieu de ne pas être balisé. Le trafic du commutateur physique provenant du VLAN natif n'est pas visible car il n'est pas balisé. Si le groupe de ports du commutateur virtuel ESXi utilise l'ID du VLAN natif, le trafic provenant des machines virtuelles sur ce port n'est pas visible pour le VLAN natif sur le commutateur, car le commutateur attend un trafic non balisé.
- Assurez-vous que les groupes de ports ne sont pas configurés sur des valeurs VLAN réservées par les commutateurs physiques en amont. Les commutateurs physiques réservent certains ID de VLAN à des fins internes, et n'autorisent souvent pas le trafic configuré sur ces valeurs. Par exemple, les commutateurs Cisco Catalyst réservent généralement les VLAN 1001 à 1024 et 4094. Utiliser un VLAN réservé peut entraîner un déni de service sur le réseau.

- Assurez-vous que les groupes de ports ne sont pas configurés sur VLAN 4095, sauf si vous utilisez le balisage d'invité virtuel (VGT). Définir un groupe de ports sur VLAN 4095 active le mode VGT. Dans ce mode, le commutateur virtuel transmet toutes les trames du réseau à la machine virtuelle sans modifier les balises VLAN , en laissant la machine virtuelle les traiter.
- Restreignez les remplacements de configuration de niveau de port sur un commutateur virtuel distribué. Les remplacements de configuration de niveau de port sont désactivés par défaut. Lorsque des remplacements sont activés, vous pouvez utiliser des paramètres de sécurité qui sont différents pour la machine virtuelle et le niveau des groupes de ports. Certaines machines virtuelles requièrent des configurations uniques, mais la surveillance est essentielle. Si les remplacements ne sont pas surveillés, n'importe quel utilisateur parvenant à accéder à une machine virtuelle avec une configuration de commutateur virtuel distribué peut tenter d'exploiter cet accès.
- Assurez-vous que le trafic en miroir du port du commutateur virtuel distribué est envoyé uniquement aux ports du collecteur ou aux VLAN autorisés. Un vSphere Distributed Switch peut mettre en miroir le trafic provenant d'un port vers un autre pour permettre aux périphériques de capture de paquets de collecter des flux de trafic spécifiques. La mise en miroir des ports envoie une copie de l'ensemble du trafic spécifié dans un format non-chiffré. Ce trafic mis en miroir contient les données complètes dans les paquets capturés, et ceci peut compromettre les données s'il est mal dirigé. Si la mise en miroir des ports est requise, vérifiez que tous les ID de VLAN, de port et de liaison montante de destination de la mise en miroir des ports sont corrects.

Étiquetage de composants de mise en réseau

L'identification des différents composants de votre architecture de mise en réseau est critique et contribue à garantir qu'aucune erreur n'est introduite lors de l'extension de votre réseau.

Suivez ces recommandations :

- Assurez-vous que les groupes de ports sont configurés avec une étiquette réseau claire et évidente. Ces étiquettes servent de descripteur fonctionnel du groupe de ports et vous aident à identifier la fonction de chaque groupe de ports lorsque le réseau devient plus complexe.
- Assurez-vous que chaque vSphere Distributed Switch dispose d'une étiquette réseau qui indique clairement la fonction ou le sous-réseau IP du commutateur. Cette étiquette sert de descripteur fonctionnel du commutateur, tout comme un commutateur physique nécessite un nom d'hôte. Par exemple, vous pouvez étiqueter le commutateur comme étant interne pour indiquer qu'il est dédié à la mise en réseau interne. Vous ne pouvez pas modifier l'étiquette d'un commutateur virtuel standard.

Documenter et vérifier l'environnement VLAN vSphere

Vérifiez votre environnement VLAN régulièrement pour éviter les problèmes. Documentez entièrement l'environnement VLAN et assurez-vous que les ID VLAN ne sont utilisés qu'une seule fois. Votre documentation peut simplifier le dépannage et est essentielle lorsque vous souhaitez développer l'environnement.

Procédure

1 Assurez-vous que tous les vSwitch et ID VLAN sont entièrement documentés

Si vous utilisez le balisage VLAN sur un commutateur virtuel, les ID doivent correspondre aux ID des commutateurs VLAN externes en amont. Si les ID VLAN ne sont pas entièrement suivis, une réutilisation erronée d'ID peut permettre l'établissement de trafic entre des machines physiques et virtuelles non appropriées. De même, si les ID VLAN sont erronés ou manquants, le trafic entre les machines physiques et virtuelles peut être bloqué à un endroit où le trafic devrait normalement passer.

2 Assurez-vous que les ID VLAN pour tous les groupes de ports virtuels distribués (instances de dvPortgroup) sont entièrement documentés

   Si vous utilisez le balisage VLAN sur un dvPortgroup, les ID doivent correspondre aux ID des commutateurs VLAN externes en amont. Si les ID VLAN ne sont pas entièrement suivis, une réutilisation erronée d'ID peut permettre l'établissement de trafic entre des machines physiques et virtuelles non appropriées. De même, si les ID VLAN sont erronés ou manquants, le trafic entre les machines physiques et virtuelles peut être bloqué à un endroit où le trafic devrait normalement passer.

3 Assurez-vous que les ID VLAN de tous les commutateurs virtuels distribués sont entièrement documentés

   Les VLAN privés (PVLAN) des commutateurs virtuels distribués nécessitent des ID VLAN principaux et secondaires. Ces ID doivent correspondre aux ID des commutateurs PVLAN externes en amont. Si les ID VLAN ne sont pas entièrement suivis, une réutilisation erronée d'ID peut permettre l'établissement de trafic entre des machines physiques et virtuelles non appropriées. De même, si des ID PVLAN sont erronés ou manquants, le trafic entre les machines physiques et virtuelles peut être bloqué là où vous souhaitez faire passer le trafic.

4 Vérifiez que les liaisons de jonction VLAN sont connectées uniquement à des ports de commutateur physiques qui fonctionnent comme des liaisons de jonction.

   Lorsque vous connectez un commutateur virtuel à un port de jonction VLAN, vous devez configurer correctement le commutateur virtuel et le commutateur physique au port de liaison montante. Si le commutateur physique n'est pas configuré correctement, les trames avec l'en-tête VLAN 802.1q sont renvoyées vers un commutateur qui n'attend par leur arrivée.

Adoption de solides pratiques d'isolation de réseau

L'adoption de solides pratiques d'isolation réseau améliore de façon significative la sécurité réseau de l'environnement vSphere.

Isoler le réseau de gestion

Le réseau de gestion vSphere donne accès à l'interface de gestion vSphere sur chaque composant. Les services s'exécutant sur l'interface de gestion offrent la possibilité pour un pirate d'obtenir un accès privilégié aux systèmes. Les attaques à distance sont susceptibles de commencer par l'obtention d'un accès à ce réseau. Si un pirate obtient accès au réseau de gestion, cela lui fournit une base pour mener d'autres intrusions.

Contrôlez strictement l'accès au réseau de gestion en le protégeant au niveau de sécurité de la machine virtuelle la plus sécurisée s'exécutant sur un hôte ou un cluster ESXi. Quelle que soit la restriction du réseau de gestion, les administrateurs doivent avoir accès à ce réseau pour configurer les hôtes ESXi et le système vCenter Server.

Placez le groupe de ports de gestion vSphere dans un VLAN dédié sur un commutateur commun. vSwitch peut être partagé avec le trafic de production (machine virtuelle), à condition que le VLAN du groupe de ports de gestion de vSphere ne soit pas utilisé par les machines virtuelles de production. Vérifiez que le segment réseau n'est pas routé, à l'exception éventuellement des réseaux hébergeant d'autres entités de gestion, par exemple en liaison avec vSphere Replication. Assurez-vous notamment que le trafic des machines virtuelles de production ne peut pas être routé vers ce réseau.

Autorisez l'accès à la fonctionnalité de gestion d'une manière strictement contrôlée en utilisant l'une des approches suivantes.

- Pour les environnements particulièrement sensibles, configurez une passerelle contrôlée ou une autre méthode contrôlée pour accéder au réseau de gestion. Par exemple, obligez les administrateurs à se connecter au réseau de gestion via un réseau VPN, et autorisez l'accès uniquement aux administrateurs approuvés.
- Configurez des systèmes JumpBox qui exécutent des clients de gestion.

Isoler le trafic de stockage

Assurez-vous que le trafic de stockage IP est isolé. Le stockage IP inclut iSCSI et NFS. Les machines virtuelles peuvent partager des commutateurs virtuels et des VLAN avec des configurations de stockage IP. Ce type de configuration peut exposer du trafic de stockage IP à des utilisateurs de machine virtuelle non autorisés.

Le stockage IP est fréquemment non chiffré ; toute personne ayant accès à ce réseau peut le voir. Pour empêcher les utilisateurs non autorisés à voir le trafic de stockage IP, séparez logiquement le trafic du réseau de stockage IP du trafic de production. Configurez les adaptateurs de stockage IP sur des VLAN ou des segments de réseau séparés du réseau de gestion VMkernel pour empêcher les utilisateurs non autorisés d'afficher le trafic.

Isoler le trafic VMotion

Les informations de migration VMotion sont transmises en texte brut. Toute personne ayant accès au réseau sur lequel ces informations circulent peut les voir. Les pirates potentiels peuvent intercepter du trafic vMotion pour obtenir le contenu de la mémoire d'une machine virtuelle. Ils peuvent également préparer une attaque MiTM dans laquelle le contenu est modifié pendant la migration.

Séparez le trafic VMotion du trafic de production sur un réseau isolé. Configurez le réseau de manière qu'il soit non routable, c'est-à-dire assurez-vous qu'aucun routeur de niveau 3 n'étend ce réseau et d'autres réseaux, pour empêcher un accès au réseau de l'extérieur.

Le groupe de ports VMotion doit se trouver dans un réseau VLAN dédié sur un vSwitch commun. vSwitch peut être partagé avec le trafic de production (machine virtuelle), à condition que le VLAN du groupe de ports VMotion ne soit pas utilisé par des machines virtuelles de production.

Utiliser des commutateurs virtuels avec vSphere Network Appliance API, uniquement si nécessaire

Si vous n'utilisez pas de produits faisant appel à vSphere Network Appliance API (DvFilter), ne configurez pas votre hôte pour envoyer des informations sur le réseau à une machine virtuelle. Si vSphere Network Appliance API est activée, un pirate peut tenter de connecter une machine virtuelle au filtre. Cette connexion risque de donner à d'autres machines virtuelles sur l'hôte un accès au réseau.

Si vous utilisez un produit qui fait appel à cette API, vérifiez que l'hôte est correctement configuré. Reportez-vous aux sections sur DvFilter dans *Développement et déploiement des solutions vSphere, des vServices et des agents ESX*. Si votre hôte est configuré pour utiliser l'API, assurez-vous que la valeur du paramètre `Net.DVFilterBindIpAddress` correspond au produit qui utilise l'API.

Procédure

1 Connectez-vous à vSphere Web Client.

2 Sélectionnez l'hôte et cliquez sur **Configurer**.

3 Dans Système, sélectionnez **Paramètres système avancés**.

4 Faites défiler jusqu'à `Net.DVFilterBindIpAddress` et vérifiez que le paramètre a une valeur vide.

L'ordre des paramètres n'est pas strictement alphabétique. Tapez **`DVFilter`** dans le champ Filtre pour afficher tous les paramètres associés.

5 Vérifiez le paramètre.

- Si vous n'utilisez pas les paramètres DvFilter, assurez-vous que la valeur est vide.
- Si vous utilisez des paramètres DvFilter, assurez-vous que la valeur du paramètre correspond à celle qu'emploie le produit qui utilise DvFilter.

Meilleures pratiques concernant plusieurs composants vSphere 9

Certaines meilleures pratiques en matière de sécurité, telles que la configuration de NTP dans votre environnement, affectent plusieurs composants vSphere. Tenez compte des recommandations suivantes lorsque vous configurez votre environnement.

Reportez-vous à Chapitre 3, « Sécurisation des hôtes ESXi », page 41 et à Chapitre 5, « Sécurisation des machines virtuelles », page 121 pour consulter des informations associées.

Ce chapitre aborde les rubriques suivantes :

Synchronisation des horloges sur le réseau vSphere

Assurez-vous que les horloges de tous les composants sur le réseau vSphere sont synchronisées. Si les horloges des machines de votre réseau vSphere ne sont pas synchronisées, les certificats SSL, qui sont sensibles au temps, risquent de ne pas être reconnus comme étant valides dans les communications entre les machines réseau.

Des horloges non synchronisées peuvent entraîner des problèmes d'authentification, ce qui peut causer l'échec de l'installation ou empêcher le démarrage du service vpxd de vCenter Server Appliance.

Assurez-vous que toute machine hôte Windows sur laquelle vCenter Server s'exécute est synchronisée avec le serveur NTP (Network Time Server). Voir l'article de la base de connaissances http://kb.vmware.com/kb/1318.

Pour synchroniser les horloges ESXi avec un serveur NTP, vous pouvez utiliser VMware Host Client. Pour plus d'informations sur la modification de la configuration de l'heure d'un hôte ESXi, reportez-vous à *Gestion des hôtes uniques vSphere*.

- Synchroniser les horloges ESXi avec un serveur de temps réseau page 186

  Avant d'installer vCenter Server ou de déployer vCenter Server Appliance, assurez-vous que toutes les horloges des machines de votre réseau vSphere sont synchronisées.

- Configuration des paramètres de synchronisation horaire dans vCenter Server Appliance page 186

  Vous pouvez modifier les paramètres de synchronisation horaire dans vCenter Server Appliance après le déploiement.

Synchroniser les horloges ESXi avec un serveur de temps réseau

Avant d'installer vCenter Server ou de déployer vCenter Server Appliance, assurez-vous que toutes les horloges des machines de votre réseau vSphere sont synchronisées.

Cette tâche explique comment configurer NTP depuis VMware Host Client. Vous pouvez également utiliser la commande vCLI `vicfg-ntp`. Reportez-vous à la *Référence de vSphere Command-Line Interface*.

Procédure

1 Démarrez VMware Host Client et connectez-vous à l'hôte ESXi.

2 Cliquez sur **Configurer**.

3 Sous **Système**, cliquez sur **Configuration de temps**, puis sur **Modifier**.

4 Sélectionnez **Utiliser le protocole de temps du réseau (activer le client NTP)**.

5 Dans la zone de texte Ajouter serveur NTP, saisissez l'adresse IP ou le nom de domaine complet d'un ou de plusieurs serveurs NTP avec lequel effectuer la synchronisation.

6 (Facultatif) Définissez la stratégie de démarrage et l'état du service.

7 Cliquez sur **OK**.

L'hôte se synchronise avec le serveur NTP.

Configuration des paramètres de synchronisation horaire dans vCenter Server Appliance

Vous pouvez modifier les paramètres de synchronisation horaire dans vCenter Server Appliance après le déploiement.

Lorsque vous déployez vCenter Server Appliance, vous pouvez définir la méthode de synchronisation horaire en utilisant un serveur NTP ou VMware Tools. En cas de modification de vos paramètres d'heure dans votre réseau vSphere, vous pouvez modifier vCenter Server Appliance et configurer les paramètres de synchronisation horaire à l'aide des commandes dans l'interpréteur de commande du dispositif.

Lorsque vous activez la synchronisation horaire régulière, VMware Tools définit l'heure de l'hôte sur le système d'exploitation invité.

Après la synchronisation horaire, VMware Tools vérifie toutes les minutes que les horloges des systèmes d'exploitation invité et de l'hôte correspondent toujours. Si tel n'est pas le cas, l'horloge du système d'exploitation client est synchronisé pour qu'elle corresponde à celle de l'hôte.

Un logiciel natif de synchronisation horaire, tel que Network Time Protocol (NTP), est généralement plus précis que la synchronisation horaire régulière de VMware Tools et il est donc préférable d'utiliser un tel logiciel. Vous pouvez utiliser une seule méthode de synchronisation horaire dans vCenter Server Appliance. Si vous décidez d'utiliser le logiciel natif de synchronisation horaire, la synchronisation horaire régulière de VMware Tools dans vCenter Server Appliance est désactivée, et l'inverse.

Utiliser la synchronisation de l'heure de VMware Tools

Vous pouvez configurer vCenter Server Appliance de manière à utiliser la synchronisation de l'heure de VMware Tools.

Procédure

1 Accédez à l'interpréteur de commande du dispositif et connectez-vous en tant qu'utilisateur disposant du rôle d'administrateur ou de super administrateur.

L'utilisateur par défaut ayant le rôle de super administrateur est l'utilisateur racine.

2 Exécutez la commande pour activer la synchronisation de l'heure de VMware Tools.

```
timesync.set --mode host
```

3 (Facultatif) Exécutez la commande pour vérifier que vous avez réussi à appliquer la synchronisation de l'heure de VMware Tools.

```
timesync.get
```

La commande renvoie l'indication que la synchronisation de l'heure est en mode hôte.

L'heure du dispositif est synchronisée avec celle de l'hôte ESXi.

Ajouter ou remplacer les serveurs NTP dans la configuration de vCenter Server Appliance

Pour configurer vCenter Server Appliance de manière à utiliser une synchronisation de l'heure basée sur NTP, vous devez ajouter les serveurs NTP à la configuration vCenter Server Appliance.

Procédure

1 Accédez à l'interpréteur de commande du dispositif et connectez-vous en tant qu'utilisateur disposant du rôle d'administrateur ou de super administrateur.

L'utilisateur par défaut ayant le rôle de super administrateur est l'utilisateur racine.

2 Ajoutez des serveurs NTP à la configuration de vCenter Server Appliance en exécutant la commande `ntp.server.add`.

Par exemple, exécutez la commande suivante :

```
ntp.server.add --servers IP-addresses-or-host-names
```

IP-addresses-or-host-names est une liste séparée par des virgules des adresses IP ou noms d'hôtes des serveurs NTP.

Cette commande ajoute des serveurs NTP à la configuration. Si la synchronisation horaire est basée sur un serveur NTP, le démon NTP est redémarré pour recharger les nouveaux serveurs NTP. Sinon, cette commande ajoute simplement de nouveaux serveurs NTP à la configuration NTP existante.

3 (Facultatif) Pour supprimer d'anciens serveurs NTP et les remplacer par de nouveaux dans la configuration de vCenter Server Appliance, exécutez la commande `ntp.server.set`.

Par exemple, exécutez la commande suivante :

```
ntp.server.set --servers IP-addresses-or-host-names
```

IP-addresses-or-host-names est une liste séparée par des virgules des adresses IP ou noms d'hôtes des serveurs NTP.

Cette commande supprime les anciens serveurs NTP de la configuration et définit les serveurs NTP d'entrée dans la configuration. Si la synchronisation horaire est basée sur un serveur NTP, le démon NTP est redémarré pour recharger la nouvelle configuration NTP. Sinon, cette commande remplace simplement les serveurs de la configuration NTP avec les serveurs que vous fournissez.

4 (Facultatif) Exécutez la commande pour vérifier que vous avez appliqué les nouveaux paramètres de la configuration NTP.

```
ntp.get
```

La commande renvoie une liste séparée par des espaces des serveurs configurés pour la synchronisation NTP. Si la synchronisation NTP est activée, la commande renvoie l'information précisant que la configuration NTP a l'état Actif. Si la synchronisation NTP est désactivée, la commande renvoie l'information précisant que la configuration NTP a l'état Inactif.

Suivant

Si la synchronisation NTP est désactivée, vous pouvez configurer les paramètres de synchronisation de l'heure de vCenter Server Appliance de façon à la baser sur un serveur NTP. Reportez-vous à « Synchroniser l'heure dans vCenter Server Appliance avec un serveur NTP », page 188.

Synchroniser l'heure dans vCenter Server Appliance avec un serveur NTP

Vous pouvez configurer les paramètres de synchronisation de l'heure dans vCenter Server Appliance pour qu'ils soient basés sur un serveur NTP.

Prérequis

Configurez un ou plusieurs serveurs NTP (Network Time Protocol) dans la configuration de vCenter Server Appliance. Reportez-vous à « Ajouter ou remplacer les serveurs NTP dans la configuration de vCenter Server Appliance », page 187.

Procédure

1 Accédez à l'interpréteur de commande du dispositif et connectez-vous en tant qu'utilisateur disposant du rôle d'administrateur ou de super administrateur.

   L'utilisateur par défaut ayant le rôle de super administrateur est l'utilisateur racine.

2 Exécutez la commande pour activer la synchronisation de l'heure basée sur un serveur NTP.

```
timesync.set --mode NTP
```

3 (Facultatif) Exécutez la commande pour vérifier que vous avez appliqué la synchronisation NTP.

```
timesync.get
```

   La commande renvoie l'indication que la synchronisation de l'heure est en mode NTP.

Meilleures pratiques en matière de sécurité du stockage

Suivez les recommandations relatives à la sécurité de stockage, présentées par votre fournisseur de sécurité de stockage. Vous pouvez également tirer avantage du CHAP et du CHAP mutuel pour sécuriser le stockage iSCSI, masquer et affecter les ressources SAN, et configurer les informations d'identification Kerberos pour NFS 4.1.

Reportez-vous également à la documentation *Administration de VMware Virtual SAN*.

Sécurisation du stockage iSCSI

Le stockage que vous configurez pour un hôte peut comprendre un ou plusieurs réseaux de zone de stockage (SAN) utilisant iSCSI. Lorsque vous configurez iSCSI sur un hôte, vous pouvez prendre plusieurs mesures pour réduire les risques de sécurité.

iSCSI est un moyen d'accéder aux périphériques SCSI et d'échanger des enregistrements de données à l'aide du protocole TCP/IP sur un port réseau plutôt que via une connexion directe à un périphérique SCSI. Dans les transactions iSCSI, des blocs de données SCSI brutes sont encapsulés dans des enregistrements iSCSI et transmis au périphérique demandant ou à l'utilisateur.

Les SAN iSCSI vous permettent d'utiliser efficacement les infrastructures Ethernet existantes pour permettre aux hôtes d'accéder aux ressources de stockage qu'ils peuvent partager de manière dynamique. Les SAN iSCSI offrent une solution de stockage économique pour les environnements reposant sur un pool de stockage pour servir de nombreux utilisateurs. Comme pour tout système en réseau, vos SAN iSCSI peuvent être soumis à des défaillances de sécurité.

Remarque Les contraintes et les procédures de sécurisation d'un SAN iSCSI sont semblables à celles des adaptateurs iSCSI matériels que vous pouvez utiliser avec les hôtes et à celles des iSCSI configurés directement via l'hôte.

Sécurisation des périphériques iSCSI

Un moyen permettant de sécuriser les périphériques iSCSI des intrusions indésirables consiste à demander que l'hôte, ou l'initiateur, soit authentifié par le périphérique iSCSI, ou la cible, à chaque fois que l'hôte tente d'accéder aux données sur la LUN cible.

L'objectif de l'authentification consiste à prouver que l'initiateur a le droit d'accéder à une cible, ce droit étant accordé lorsque vous configurez l'authentification.

ESXi ne prend en charge ni Secure Remote Protocol (SRP), ni les méthodes d'authentification par clé publique d'iSCSI. L'authentification Kerberos ne peut s'utiliser qu'avec NFS 4.1.

ESXi prend en charge l'authentification CHAP ainsi que l'authentification CHAP mutuel. La documentation *Stockage vSphere* explique comment sélectionner la meilleure méthode d'authentification pour votre périphérique iSCSI et comment configurer CHAP.

Assurez-vous que le secrets CHAP sont uniques. Le secret d'authentification mutuelle de chaque hôte doit être différent. Dans la mesure du possible, le secret doit également être différent pour chaque client s'authentifiant auprès du serveur. De la sorte, si un hôte unique est compromis, le pirate ne peut pas créer un autre hôte arbitraire et s'authentifier auprès du périphérique de stockage. Lorsqu'il existe un secret partagé unique, la compromission d'un hôte peut permettre à un pirate de s'authentifier auprès du périphérique de stockage.

Protection d'un SAN iSCSI

Lorsque vous planifiez la configuration iSCSI, prenez des mesures pour optimiser la sécurité globale de votre SAN iSCSI. Votre configuration iSCSI présente le même niveau de sécurité que votre réseau IP. Par conséquent, en appliquant de bonnes normes de sécurité lors de la configuration de votre réseau, vous aidez à la protection de votre stockage iSCSI.

Vous trouverez ci-dessous des suggestions spécifiques pour appliquer de bonnes normes de sécurité.

Protection des données transmises

Le premier risque de sécurité dans les SAN iSCSI est qu'un attaquant puisse renifler les données de stockage transmises.

Prenez des mesures supplémentaires pour empêcher les attaquants de voir aisément les données iSCSI. Ni l'adaptateur iSCSI du matériel, ni l'initiateur iSCSI d'ESXi ne chiffre les données qu'ils transmettent vers les cibles et obtiennent de celles-ci, rendant ainsi les données plus vulnérables aux attaques par reniflage.

Permettre à vos machines virtuelles de partager des commutateurs standard et des VLAN avec votre configuration iSCSI expose potentiellement le trafic iSCSI à une mauvaise utilisation par un attaquant de machine virtuelle. Afin de garantir que les intrus ne peuvent pas écouter les transmissions iSCSI, assurez-vous qu'aucune des machines virtuelles ne peut voir le réseau de stockage iSCSI.

Si vous utilisez un adaptateur iSCSI matériel, vous pouvez effectuer cette opération en vous assurant que l'adaptateur iSCSI et l'adaptateur de réseau physique ESXi ne sont pas connectés par inadvertance en dehors de l'hôte pour partager un commutateur ou un autre élément. Si vous configurez iSCSI directement via l'hôte ESXi, vous pouvez effectuer cette opération en configurant le stockage iSCSI via un commutateur standard différent de celui utilisé par vos machines virtuelles.

En plus de protéger le SAN iSCSI en lui attribuant un commutateur standard, vous pouvez configurer votre SAN iSCSI avec son propre VLAN pour améliorer les performances et la sécurité. Le placement de votre configuration iSCSI sur un VLAN séparé garantit qu'aucun périphérique autre que l'adaptateur iSCSI n'a de visibilité sur les transmissions au sein du SAN iSCSI. Par conséquent, aucun blocage réseau provenant d'autres sources ne peut interférer avec le trafic iSCSI.

Sécurisation des ports iSCSI

Lorsque vous exécutez des périphériques iSCSI, ESXi n'ouvre pas de port écoutant les connexions réseau. Cette mesure réduit le risque qu'un intrus puisse pénétrer dans ESXi par des ports disponibles et prenne le contrôle de l'hôte. Par conséquent, l'exécution iSCSI ne présente pas de risques de sécurité supplémentaires sur le côté hôte ESXi de la connexion.

Tout périphérique cible iSCSI que vous exécutez doit disposer d'un ou plusieurs ports TCP ouverts pour écouter les connexions iSCSI. Si des vulnérabilités de sécurité existent dans le logiciel du périphérique iSCSI, vos données peuvent courir un risque en raison d'une panne d'ESXi. Pour réduire ce risque, installez tous les correctifs de sécurité que le fournisseur de votre équipement de stockage fournit et limitez le nombre de périphériques connectés au réseau iSCSI.

Masquage et zonage des ressources SAN

Vous pouvez utiliser le zonage et le masquage LUN pour distinguer l'activité SAN et restreindre l'accès aux périphériques de stockage.

Vous pouvez protéger l'accès au stockage dans votre environnement vSphere en utilisant le zonage et le masquage LUN avec vos ressources SAN. Par exemple, vous pouvez gérer des zones définies pour des tests indépendamment dans le réseau SAN afin qu'elles n'interfèrent pas avec l'activité des zones de production. De même, vous pouvez configurer différentes zones pour différents services.

Lorsque vous configurez des zones, tenez compte des groupes d'hôtes qui sont configurés sur le périphérique SAN.

Les possibilités de zonage et de masquage pour chaque commutateur et baie de disques SAN, ainsi que les outils de gestion du masquage LUN sont spécifiques du fournisseur.

Consultez la documentation de votre fournisseur SAN ainsi que la documentation *Stockage vSphere*.

Utilisation de Kerberos pour NFS 4.1

Avec NFS version 4.1, ESXi prend en charge le mécanisme d'authentification Kerberos.

Le mécanisme Kerberos RPCSEC_GSS est un service d'authentification. Il permet à un client NFS 4.1 installé sur ESXi de justifier son identité à un serveur NFS, préalablement au montage d'un partage NFS. Grâce au chiffrement, la sécurité Kerberos permet de travailler sur une connexion réseau non sécurisée.

La mise en œuvre ESXi de Kerberos pour NFS 4.1 fournit deux modèles de sécurité, krb5 et krb5i, qui offrent deux niveaux de sécurité différents.

- Kerberos pour l'authentification uniquement (krb5) prend en charge la vérification de l'identité.
- Kerberos pour l'authentification et l'intégrité des données (krb5i), en plus de la vérification de l'identité, fournit des services d'intégrité des données. Ces services permettent de protéger le trafic NFS contre la falsification en vérifiant les modifications potentielles des paquets de données.

Kerberos prend en charge des algorithmes de chiffrement qui empêchent les utilisateurs non autorisés d'obtenir l'accès au trafic NFS. Le client NFS 4.1 sur ESXi tente d'utiliser l'algorithme AES256-CTS-HMAC-SHA1-96 ou AES128-CTS-HMAC-SHA1-96 pour accéder à un partage sur le serveur NAS. Avant d'utiliser vos banques de données NFS 4.1, assurez-vous que l'algorithme AES256-CTS-HMAC-SHA1-96 ou AES128-CTS-HMAC-SHA1-96 est activé sur le serveur NAS.

Le tableau suivant compare les niveaux de sécurité Kerberos pris en charge par ESXi.

Tableau 9-1. Types de sécurité Kerberos

		ESXi 6.0	ESXi 6.5
Kerberos pour l'authentification uniquement (krb5)	Total de contrôle d'intégrité pour l'en-tête RPC	Oui avec DES	Oui avec AES
	Total de contrôle d'intégrité pour les données RPC	Non	Non
Kerberos pour l'authentification et l'intégrité des données (krb5i)	Total de contrôle d'intégrité pour l'en-tête RPC	Pas de krb5i	Oui avec AES
	Total de contrôle d'intégrité pour les données RPC		Oui avec AES

Lorsque vous utilisez l'authentification Kerberos, les considérations suivantes s'appliquent :

- ESXi utilise Kerberos avec le domaine Active Directory.
- En tant qu'administrateur de vSphere, vous devez spécifier les informations d'identification Active Directory requises pour octroyer l'accès aux banques de données Kerberos NFS 4.1 à un utilisateur NFS. Le même ensemble d'informations d'identification est utilisé pour accéder à toutes les banques de données Kerberos montées sur cet hôte.
- Lorsque plusieurs hôtes ESXi partagent la même banque de données NFS 4.1, vous devez utiliser les mêmes informations d'identification Active Directory pour tous les hôtes qui accèdent à la banque de données partagée. Pour automatiser le processus d'attribution, définissez l'utilisateur dans un profil d'hôte et appliquez le profil à tous les hôtes ESXi.
- Vous ne pouvez pas utiliser deux mécanismes de sécurité, AUTH_SYS et Kerberos, pour la même banque de données NFS 4.1 partagée par plusieurs hôtes.

Pour des instructions détaillées, reportez-vous à la documentation *Stockage vSphere*.

Vérifier que l'envoi des données de performances de l'hôte aux invités est désactivé

vSphere comprend des compteurs de performance de machine virtuelle lorsque VMware Tools est installé sous des systèmes d'exploitation Windows. Les compteurs de performance permettent aux personnes en charge des machines virtuelles d'effectuer des analyses de performance précises à l'intérieur du système d'exploitation client. Par défaut, vSphere n'expose pas les informations relatives à l'hôte à la machine virtuelle invitée.

La possibilité d'envoyer des données de performance relatives à l'hôte à une machine virtuelle cliente est désactivée par défaut. Ce paramétrage par défaut empêche une machine virtuelle d'obtenir des informations détaillées sur l'hôte physique et rend les données de l'hôte indisponibles si une faille de la sécurité de la machine virtuelle se produit.

Remarque La procédure ci-dessous illustre le processus simple. Utilisez plutôt l'une des interfaces de ligne de commande vSphere (vCLI, PowerCLI et ainsi de suite) pour effectuer cette tâche sur tous les hôtes simultanément.

Procédure

1 Sur le système ESXi hébergeant la machine virtuelle, accédez au fichier VMX.

Les fichiers de configuration des machines virtuelles se situent dans le répertoire `/vmfs/volumes/datastore`, où *datastore* correspond au nom du périphérique de stockage dans lequel sont stockés les fichiers de la machine virtuelle.

2 Dans le fichier VMX, vérifiez que le paramètre suivant est défini.

```
tools.guestlib.enableHostInfo=FALSE
```

3 Enregistrez et fermez le fichier.

Vous ne pouvez pas récupérer d'informations de performance relatives à l'hôte à l'intérieur de la machine virtuelle.

Configuration de délais d'expiration pour ESXi Shell et vSphere Web Client

Pour empêcher des intrus d'utiliser une session inactive, veillez à configurer des délais d'expiration pour ESXi Shell et vSphere Web Client.

Délai d'expiration d' ESXi Shell

Pour ESXi Shell, vous pouvez configurer les délais d'expiration suivants pour vSphere Web Client à partir de l'interface utilisateur de console directe (DCUI).

Délai d'expiration de la disponibilité — La valeur du délai d'attente de disponibilité correspond au temps qui peut s'écouler avant de vous connecter suite à l'activation de ESXi Shell. Lorsque le délai est écoulé, le service est désactivé et les utilisateurs ne peuvent plus se connecter.

Délai d'inactivité — Le délai d'inactivité correspond au temps qui peut s'écouler avant que l'utilisateur ne soit déconnecté d'une session interactive inactive. Les modifications du délai d'inactivité s'appliquent lors de la prochaine connexion de l'utilisateur à ESXi Shell. Les modifications n'ont pas d'incidence sur les sessions existantes.

Délai d'expiration de vSphere Web Client

Par défaut, les sessions vSphere Web Client prennent fin après 120 minutes. Vous pouvez modifier ce paramètre par défaut dans le fichier `webclient.properties`, ainsi que cela est indiqué dans la documentation *Gestion de vCenter Server et des hôtes*.

Privilèges définis

10

Les tableaux suivants présentent les privilèges par défaut qui, une fois sélectionnés pour un rôle, peuvent être associés avec un utilisateur et assignés à un objet. Dans les tableaux de cette annexe, VC désigne vCenter Server et HC désigne le client de l'hôte, un hôte ESXi autonome ou un hôte de poste de travail.

En définissant des autorisations, vérifiez que tous les types d'objet sont définis avec des privilèges appropriés pour chaque action particulière. Quelques opérations exigent la permission d'accès au dossier racine ou au dossier parent en plus de l'accès à l'objet manipulé. Quelques opérations exigent l'autorisation d'accès ou de performances à un dossier parent et à un objet associé.

Les extensions de vCenter Server peuvent définir des privilèges supplémentaires non mentionnés ici. Référez-vous à la documentation concernant l'extension pour plus d'informations sur ces privilèges.

Ce chapitre aborde les rubriques suivantes :

Privilèges d'alarmes

Les privilèges d'alarmes contrôlent la capacité à créer et à modifier des alarmes sur des objets d'inventaire, et à y répondre.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-1. Privilèges d'alarmes

Nom de privilège	Description	Requis sur
Alarmes.Reconnaître une alarme	Permet la suppression de toutes les actions d'alarme sur toutes les alarmes déclenchées.	Objet sur lequel une alarme est définie
Alarmes.Créer une alarme	Permet la création d'une alarme. En créant des alarmes avec une action personnalisée, le privilège d'exécuter l'action est vérifié quand l'utilisateur crée l'alarme.	Objet sur lequel une alarme est définie
Alarmes.Désactiver une action d'alarme	Permet d'empêcher une action d'alarme après le déclenchement d'une alarme. Cette intervention ne désactive pas l'alarme.	Objet sur lequel une alarme est définie

Tableau 10-1. Privilèges d'alarmes (suite)

Nom de privilège	Description	Requis sur
Alarmes.Modifier une alarme	Permet le changement des propriétés d'une alarme.	Objet sur lequel une alarme est définie
Alarmes.Supprimer une alarme	Permet la suppression d'une alarme.	Objet sur lequel une alarme est définie
Alarmes.Définir un état d'alarme	Permet de changer l'état de l'alarme d'événement configurée. L'état peut changer en **Normal**, **Avertissement** ou **Alerte**.	Objet sur lequel une alarme est définie

Privilèges Auto Deploy et privilèges de profil d'image

Les privilèges Auto Deploy contrôlent qui peut effectuer différentes tâches sur les règles Auto Deploy et qui peut associer un hôte. Ils permettent également de contrôler qui peut créer ou modifier un profil d'image.

Le tableau suivant décrit les privilèges qui déterminent les personnes pouvant gérer les règles et les ensembles de règles Auto Deploy et celles qui peuvent créer et modifier des profils d'image. Voir *Installation et configuration de vSphere*.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-2. Privilèges Auto Deploy

Nom de privilège	Description	Requis sur
Auto Deploy.Hôte.Associer une machine	Permet aux utilisateurs d'exécuter une commande PowerCLI qui associe un hôte à une machine.	vCenter Server
Auto Deploy.Profil d'image.Créer	Permet de créer des profils d'image.	vCenter Server
Auto Deploy.Profil d'image.Modifier	Permet de modifier des profils d'image.	vCenter Server
Auto Deploy.Règle.Créer	Permet de créer des règles Auto Deploy.	vCenter Server
Auto Deploy.Règle.Supprimer	Permet de supprimer des règles Auto Deploy.	vCenter Server
Auto Deploy.Règle.Modifier	Permet de modifier des règles Auto Deploy.	vCenter Server
Auto Deploy.Ensemble de règles.Activer	Permet d'activer des ensembles de règles Auto Deploy.	vCenter Server
Auto Deploy.Ensemble de règles.Modifier	Permet de modifier des ensembles de règles Auto Deploy.	vCenter Server

Privilèges de certificats

Les privilèges de certificats déterminent les utilisateurs pouvant gérer les certificats d'ESXi.

Ce privilège détermine qui peut effectuer la gestion de certificats pour les hôtes ESXi. Pour obtenir plus d'informations sur la gestion des certificats vCenter Server, reportez-vous à la section Privilèges requis pour les opérations de gestion des certificats dans la documentation *Administration de Platform Services Controller* .

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-3. Privilèges de certificats d'hôte

Nom de privilège	Description	Requis sur
Certificats.Gérer des certificats	Permet la gestion de certificats pour les hôtes ESXi.	vCenter Server

Privilèges de bibliothèque de contenu

Les bibliothèques de contenu offrent une méthode simple et efficace pour gérer les modèles de machines virtuelles et les vApp. Les privilèges de bibliothèque de contenu contrôlent qui peut afficher ou gérer les différents aspects des bibliothèques de contenu.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-4. Privilèges de bibliothèque de contenu

Nom de privilège	Description	Requis sur
Bibliothèque de contenu.Ajouter un élément de bibliothèque	Autorise l'ajout d'éléments à une bibliothèque.	Bibliothèque
Bibliothèque de contenu.Créer une bibliothèque locale	Autorise la création de bibliothèques locales sur le système vCenter Server spécifié.	vCenter Server
Bibliothèque de contenu.Créer une bibliothèque abonnée	Autorise la création de bibliothèques abonnées.	vCenter Server
Bibliothèque de contenu.Supprimer un élément de bibliothèque	Autorise la suppression d'éléments de bibliothèque.	Bibliothèque. Configurez cette autorisation pour qu'elle se propage à tous les éléments de la bibliothèque.
Bibliothèque de contenu.Supprimer une bibliothèque locale	Autorise la suppression d'une bibliothèque locale.	Bibliothèque
Bibliothèque de contenu.Supprimer une bibliothèque abonnée	Autorise la suppression d'une bibliothèque abonnée.	Bibliothèque
Bibliothèque de contenu.Télécharger des fichiers	Autorise le téléchargement de fichiers de la bibliothèque de contenu.	Bibliothèque
Bibliothèque de contenu.Expulser un élément de bibliothèque	Autorise l'éviction d'éléments. Le contenu d'une bibliothèque abonnée peut être mis en cache ou non. S'il est mis en cache, vous pouvez libérer un élément de la bibliothèque en l'expulsant (si vous disposez de ce privilège).	Bibliothèque. Configurez cette autorisation pour qu'elle se propage à tous les éléments de la bibliothèque.
Bibliothèque de contenu.Expulser une bibliothèque abonnée	Autorise l'éviction d'une bibliothèque abonnée. Le contenu d'une bibliothèque abonnée peut être mis en cache ou non. S'il est mis en cache, vous pouvez libérer une bibliothèque en l'expulsant (si vous disposez de ce privilège).	Bibliothèque

Tableau 10-4. Privilèges de bibliothèque de contenu (suite)

Nom de privilège	Description	Requis sur
Bibliothèque de contenu.Importer un stockage	Autorise un utilisateur à importer un élément de bibliothèque si l'URL du fichier source commence par ds:// ou file://. Ce privilège est désactivé pour l'administrateur de bibliothèque de contenu par défaut. Comme une importation à partir d'une URL de stockage implique une importation de contenu, n'activez ce privilège qu'en cas de besoin et s'il n'existe aucun problème de sécurité concernant l'utilisateur qui va effectuer l'importation.	Bibliothèque
Bibliothèque de contenu.Contrôler les informations sur l'abonnement	Ce privilège autorise les utilisateurs de solution et les API à contrôler les informations d'abonnement d'une bibliothèque distante (URL, certificat SSL et mot de passe, notamment). La structure obtenue indique si la configuration de l'abonnement s'est bien déroulée ou si des problèmes se sont produits (des erreurs SSL, par exemple).	Bibliothèque
Bibliothèque de contenu.Stockage de lecture	Autorise la lecture du stockage d'une bibliothèque de contenu.	Bibliothèque
Bibliothèque de contenu.Synchroniser l'élément de la bibliothèque	Autorise la synchronisation des éléments de bibliothèque.	Bibliothèque. Configurez cette autorisation pour qu'elle se propage à tous les éléments de la bibliothèque.
Bibliothèque de contenu.Synchroniser la bibliothèque abonnée	Autorise la synchronisation des bibliothèques abonnées.	Bibliothèque
Bibliothèque de contenu.Introspection de type	Autorise un utilisateur de solution ou un API à examiner les plug-ins de support de type pour Content Library Service.	Bibliothèque
Bibliothèque de contenu.Mettre à jour les paramètres de configuration	Vous autorise à mettre à jour les paramètres de configuration. Aucun élément d'interface utilisateur de vSphere Web Client n'est associé à ce privilège.	Bibliothèque
Bibliothèque de contenu.Mettre à jour les fichiers	Vous autorise à télécharger le contenu dans la bibliothèque de contenu. Vous permet également de supprimer les fichiers d'un élément de bibliothèque.	Bibliothèque
Bibliothèque de contenu.Mettre à jour la bibliothèque	Permet de mettre à jour la bibliothèque de contenu.	Bibliothèque
Bibliothèque de contenu.Mettre à jour l'élément de bibliothèque	Permet de mettre à jour les éléments de bibliothèque.	Bibliothèque. Configurez cette autorisation pour qu'elle se propage à tous les éléments de la bibliothèque.
Bibliothèque de contenu.Mettre à jour la bibliothèque locale	Permet de mettre à jour les bibliothèques locales.	Bibliothèque
Bibliothèque de contenu.Mettre à jour la bibliothèque abonnée	Vous autorise à mettre à jour les propriétés d'une bibliothèque abonnée.	Bibliothèque
Bibliothèque de contenu.Afficher les paramètres de configuration	Vous autorise à afficher les paramètres de configuration. Aucun élément d'interface utilisateur de vSphere Web Client n'est associé à ce privilège.	Bibliothèque

Privilèges d'opérations de chiffrement

Les privilèges d'opérations de chiffrement contrôlent qui peut effectuer quel type d'opération de chiffrement, et sur quel type d'objet.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-5. Privilèges d'opérations de chiffrement

Nom de privilège	Description	Requis sur
Opérations de chiffrement.Accès direct	Permet aux utilisateurs d'accéder aux ressources chiffrées. Par exemple, les utilisateurs peuvent exporter les machines virtuelles, avoir un accès NFC aux machines virtuelles, etc.	Machine virtuelle, hôte ou banque de données
Opérations de chiffrement.Ajouter un disque	Permet aux utilisateurs d'ajouter un disque à une machine virtuelle chiffrée.	Machine virtuelle
Opérations de chiffrement.Cloner	Permet aux utilisateurs de cloner une machine virtuelle chiffrée.	Machine virtuelle
Opérations de chiffrement.Déchiffrer	Permet aux utilisateurs de déchiffrer une machine virtuelle ou un disque.	Machine virtuelle
Opérations de chiffrement.Chiffrer	Permet aux utilisateurs de chiffrer une machine virtuelle ou un disque de machine virtuelle.	Machine virtuelle
Opérations de chiffrement.Chiffrer un nouvel élément	Permet aux utilisateurs de chiffrer une machine virtuelle ou un disque lors de sa création.	Dossier de machine virtuelle
Opérations de chiffrement.Gérer des stratégies de chiffrement	Permet aux utilisateurs de gérer les stratégies de stockage des machines virtuelles avec des filtres d'E/S de chiffrement. Par défaut, les machines virtuelles qui utilisent la stratégie de stockage de chiffrement n'utilisent pas d'autres stratégies de stockage.	Dossier racine de vCenter Server
Opération de chiffrement.Gérer des serveurs de clés	Permet aux utilisateurs de gérer le serveur de gestion des clés (KMS) du système vCenter Server. Les tâches de gestion incluent l'ajout et la suppression d'instances de serveur de gestion des clés et l'établissement d'une relation de confiance avec ce serveur.	Système vCenter Server
Opérations de chiffrement.Gérer des clés	Permet aux utilisateurs d'effectuer des opérations de gestion des clés. Ces opérations ne sont pas prises en charge à partir du dispositif vSphere Web Client mais peuvent être effectuées en utilisant `crypto-util` ou l'API.	Dossier racine de vCenter Server

Tableau 10-5. Privilèges d'opérations de chiffrement (suite)

Nom de privilège	Description	Requis sur
Opérations de chiffrement.Migrer	Permet aux utilisateurs de migrer une machine virtuelle vers un hôte ESXi différent. Prend en charge la migration avec ou sans vMotion et Storage vMotion. Ne prend pas en charge la migration vers une autre instance de vCenter Server.	Machine virtuelle
Opérations de chiffrement.Rechiffrer	Permet aux utilisateurs de rechiffrer les machines virtuelles ou les disques avec une clé différente. Ce privilège est requis pour les opérations de rechiffrement importantes et superficielles.	Machine virtuelle
Opérations de chiffrement.Enregistrer une VM	Permet aux utilisateurs d'enregistrer une machine virtuelle auprès d'un hôte ESXi.	Dossier de machine virtuelle
Opérations de chiffrement.Enregistrer un hôte	Permet aux utilisateurs d'activer le chiffrement sur un hôte. Vous pouvez activer le chiffrement sur un hôte explicitement, ou le processus de création de machine virtuelle peut l'activer.	Dossier hôte pour les hôtes autonomes, cluster des hôtes dans le cluster

Privilèges de centre de données

Les privilèges de centre de données contrôlent la capacité à créer et modifier des centres de données dans l'inventaire vSphere Web Client.

Tous les privilèges de centre de données ne sont utilisés que dans vCenter Server. Le privilège **Créer un centre de données** est défini sur les dossiers du centre de données ou l'objet racine. Tous les autres privilèges de centre de données sont associés à des centres de données, des dossiers de centres de données ou à l'objet racine.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-6. Privilèges de centre de données

Nom de privilège	Description	Requis sur
Centre de données.Créer un centre de données	Permet de créer un centre de données.	Objet de dossier de centre de données ou objet racine
Centre de données.Déplacer un centre de données	Permet de déplacer un centre de données. Le privilège doit être présent à la fois à la source et à la destination.	Centre de données, source et destination
Centre de données.Configuration d'un profil de protocole réseau	Permet de configurer le profil réseau d'un centre de données.	Centre de données
Centre de données.Interroger une allocation de pool de requêtes IP	Permet la configuration d'un pool d'adresses IP.	Centre de données
Centre de données.Reconfigurer centre de données	Permet de reconfigurer un centre de données.	Centre de données

Tableau 10-6. Privilèges de centre de données (suite)

Nom de privilège	Description	Requis sur
Centre de données.Libérer une allocation IP	Permet de libérer l'allocation IP attribuée à un centre de données.	Centre de données
Centre de données.Supprimer centre de données	Permet de supprimer un centre de données. Pour pouvoir exécuter cette opération, ce privilège doit être assigné à la fois à l'objet et à son objet parent.	Centre de données et objet parent
Centre de données.Renommer un centre de données	Permet de modifier le nom d'un centre de données.	Centre de données

Privilèges de banque de données

Les privilèges de banque de données contrôlent la capacité à parcourir, gérer, et allouer l'espace sur les banques de données.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-7. Privilèges de banque de données

Nom de privilège	Description	Requis sur
Banque de données.Allouer de l'espace	Permet l'allocation d'espace sur une banque de données pour une machine virtuelle, un snapshot, un clone ou un disque virtuel.	Centres de données
Banque de données.Parcourir une banque de données	Permet la recherche de fichiers sur une banque de données.	Centres de données
Banque de données.Configurer une banque de données	Permet la configuration d'une banque de données.	Centres de données
Banque de données.Opérations de fichier de niveau inférieur	Permet l'exécution d'opérations de lecture, d'écriture, de suppression et de changement de nom dans le navigateur de la banque de données.	Centres de données
Banque de données.Déplacer une banque de données	Permet le déplacement d'une banque de données entre dossiers. Les privilèges doivent être présents à la fois à la source et à la destination.	La banque de données, source et destination
Banque de données.Supprimer une banque de données	Permet la suppression d'une banque de données. Ce privilège est à éviter. Pour pouvoir exécuter cette opération, un utilisateur ou un groupe d'utilisateurs doit disposer de ce privilège attribué à la fois à l'objet et à son objet parent.	Centres de données
Banque de données.Supprimer un fichier	Permet la suppression de fichiers dans la banque de données. Ce privilège est à éviter. Attribue le privilège **Opérations de fichier de niveau inférieur**.	Centres de données
Banque de données.Renommer une banque de données	Permet de renommer une banque de données.	Centres de données
Banque de données.Mettre à jour des fichiers de machine virtuelle	Permet de mettre à niveau les chemins d'accès aux fichiers de machine virtuelle sur une banque de données après que la banque de données a été resignée.	Centres de données
Banque de données.Mettre à jour des métadonnées de machine virtuelle	Permet de mettre à jour les métadonnées de la machine virtuelle associées à une banque de données.	Centres de données

Privilèges de cluster de banques de données

Les privilèges de cluster de banques de données contrôlent la configuration des clusters de banques de données du DRS de stockage.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-8. Privilèges de cluster de banques de données

Nom de privilège	Description	Requis sur
Cluster de banques de données.Configurer un cluster de banques de données	Permet la création et la configuration de paramètres pour les clusters de banques de données de Storage DRS.	Clusters de banques de données

Privilèges de Distributed Switch

Les privilèges de Distributed Switch contrôlent la capacité à effectuer des tâches associées à la gestion des instances de Distributed Switch.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-9. Privilèges de vSphere Distributed Switch

Nom de privilège	Description	Requis sur
Distributed Switch.Créer	Autorise la création d'une instance de Distributed Switch.	Centres de données, dossiers réseau
Distributed Switch.Supprimer	Autorise la suppression d'une instance de Distributed Switch. Pour pouvoir exécuter cette opération, un utilisateur ou un groupe d'utilisateurs doit disposer de ce privilège attribué à la fois à l'objet et à son objet parent.	Distributed switches
Distributed Switch.Opération de l'hôte	Autorise le changement des membres hôtes d'une instance de Distributed Switch.	Distributed switches
Distributed Switch.Modifier	Autorise la modification de la configuration d'une instance de Distributed Switch.	Distributed switches
Distributed Switch.Déplacer	Autorise le déplacement d'un vSphere Distributed Switch vers un autre dossier.	Distributed switches
Distributed Switch.Opération de Network I/O control	Autorise la modification des paramètres de ressources d'un vSphere Distributed Switch.	Distributed switches
Distributed Switch.Opération de stratégie	Autorise la modification de la règle d'un vSphere Distributed Switch.	Distributed switches
Distributed Switch .Opération de configuration de port	Autorise la modification de la configuration d'un port dans un vSphere Distributed Switch.	Distributed switches

Tableau 10-9. Privilèges de vSphere Distributed Switch (suite)

Nom de privilège	Description	Requis sur
Distributed Switch.Opération de définition de port	Autorise la modification des paramètres d'un port dans un vSphere Distributed Switch.	Distributed switches
Distributed Switch.Opération VSPAN	Autorise la modification de la configuration VSPAN d'un vSphere Distributed Switch.	Distributed switches

Privilèges de gestionnaire d'agent ESX

Les privilèges de gestionnaire d'agent ESX contrôlent les opérations liées au Gestionnaire d'agent ESX et aux machines virtuelles d'agent. Le gestionnaire d'agent ESX est un service qui vous permet d'installer des machines virtuelles de gestion liées à un hôte et non affectées par VMware DRS ou d'autres services qui migrent des machines virtuelles.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-10. Gestionnaire d'agent ESX

Nom de privilège	Description	Requis sur
ESX Agent Manager.Configuration	Permet de déployer une machine virtuelle d'agent sur un hôte ou un cluster.	Machines virtuelles
ESX Agent Manager.Modifier	Permet d'apporter des modifications à une machine virtuelle d'agent telles que la mise hors tension ou la suppression de la machine virtuelle.	Machines virtuelles
ESX Agent View.Afficher	Permet d'afficher une machine virtuelle d'agent.	Machines virtuelles

Privilèges d'extension

Les privilèges d'extension contrôlent la capacité à installer et gérer des extensions.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-11. Privilèges d'extension

Nom de privilège	Description	Requis sur
Extension.Enregistrer une extension	Permet d'enregistrer une extension (plug-in).	Instance racine de vCenter Server
Extension.Annuler l'enregistrement d'une extension	Permet d'annuler l'enregistrement d'une extension (plug-in).	Instance racine de vCenter Server
Extension.Mettre à jour une extension	Permet de mettre à jour une extension (plug-in).	Instance racine de vCenter Server

Privilèges de dossier

Les privilèges de dossier contrôlent la capacité à créer et gérer des dossiers.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-12. Privilèges de dossier

Nom de privilège	Description	Requis sur
Dossier.Créer un dossier	Permet de créer un dossier.	Dossiers
Dossier.Supprimer un dossier	Permet de supprimer un dossier. Pour pouvoir exécuter cette opération, un utilisateur ou un groupe d'utilisateurs doit disposer de ce privilège attribué à la fois à l'objet et à son objet parent.	Dossiers
Dossier.Déplacer un dossier	Permet de déplacer un dossier. Le privilège doit être présent à la fois à la source et à la destination.	Dossiers
Dossier.Renommer un dossier	Permet de modifier le nom d'un dossier.	Dossiers

Privilèges globaux

Les privilèges globaux contrôlent un certain nombre de tâches globales associées aux tâches, aux scripts et aux extensions.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-13. Privilèges globaux

Nom de privilège	Description	Requis sur
Global.Agir en tant que vCenter Server	Permet la préparation ou le lancement d'une opération d'envoi vMotion ou d'une opération de réception vMotion.	Instance racine de vCenter Server
Global.Annuler une tâche	Permet l'annulation d'une tâche en cours d'exécution ou en file d'attente.	Objet d'inventaire associé à la tâche
Global.Planification de capacité	Permet l'activation de l'utilisation de la planification de capacité pour prévoir la consolidation de machines physiques en machines virtuelles.	Instance racine de vCenter Server
Global.Diagnostics	Permet la récupération d'une liste de fichiers de diagnostic, d'un en-tête de journal, de fichiers binaires ou d'un groupe de diagnostic. Pour éviter d'éventuelles failles de sécurité, limitez ce privilège au rôle d'administrateur vCenter Server.	Instance racine de vCenter Server
Global.Désactiver des méthodes	Permet à des serveurs d'extensions de vCenter Server de désactiver des opérations sur des objets gérés par vCenter Server.	Instance racine de vCenter Server
Global.Activer des méthodes	Permet aux serveurs d'extensions vCenter Server d'activer certaines opérations sur des objets gérés par vCenter Server.	Instance racine de vCenter Server
Global.Balise globale	Permet l'ajout ou la suppression de balises globales.	Hôte racine ou instance racine de vCenter Server
Global.Santé	Permet l'affichage de l'état de fonctionnement de composants de vCenter Server.	Instance racine de vCenter Server

Tableau 10-13. Privilèges globaux (suite)

Nom de privilège	Description	Requis sur
Global.Licences	Permet l'affichage de licences installées, ainsi que l'ajout ou la suppression de licences.	Hôte racine ou instance racine de vCenter Server
Global.Événement de journal	Permet la consignation d'un événement défini par l'utilisateur par rapport à une entité gérée.	Tout objet
Global.Gérer des attributs personnalisés	Permet d'ajouter, de supprimer ou de renommer des définitions de champs personnalisés.	Instance racine de vCenter Server
Global.Proxy	Permet l'accès à une interface interne pour ajouter ou supprimer des points finaux à ou depuis un proxy.	Instance racine de vCenter Server
Global.Action de script	Permet de planifier une action de script en relation avec une alarme.	Tout objet
Global.Gestionnaires de services	Permet l'utilisation de la commande `resxtop` dans l'interface de ligne de commande vSphere.	Hôte racine ou instance racine de vCenter Server
Global.Définir un attribut personnalisé	Permet de visualiser, créer ou supprimer des attributs personnalisés pour un objet géré.	Tout objet
Global.Paramètres	Permet la lecture ou la modification de paramètres de configuration d'exécution de vCenter Server.	Instance racine de vCenter Server
Global.Balise système	Permet l'ajout ou la suppression de balises système.	Instance racine de vCenter Server

Privilèges CIM d'hôte

Les privilèges d'hôte CIM contrôlent l'utilisation du CIM pour la surveillance de la santé de l'hôte.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-14. Privilèges CIM d'hôte

Nom de privilège	Description	Requis sur
Hôte.CIM.Interaction CIM	Permettre à un client d'obtenir un billet pour l'utilisation de services CIM.	Hôtes

Privilèges de configuration d'hôte

Les privilèges de configuration d'hôte contrôlent la capacité à configurer des hôtes.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-15. Privilèges de configuration d'hôte

Nom de privilège	Description	Requis sur
Hôte.Configuration.Paramètres avancés	Permet de définir des options avancées de configuration d'hôte.	Hôtes
Hôte.Configuration.Banque d'authentification	Permet de configurer les banques d'authentification d'Active Directory.	Hôtes
Hôte.Configuration.Modifier les paramètres PciPassthru	Permet de modifier les paramètres PciPassthru pour un hôte.	Hôtes

Tableau 10-15. Privilèges de configuration d'hôte (suite)

Nom de privilège	Description	Requis sur
Hôte.Configuration.Modifier les paramètres SNMP	Permet de modifier les paramètres SNMP d'un hôte.	Hôtes
Hôte.Configuration.Modifier les paramètres de date et heure	Permet de modifier les paramètres de date et d'heure sur l'hôte.	Hôtes
Hôte.Configuration.Modifier les paramètres	Permet de paramétrer le mode verrouillage sur des hôtes ESXi.	Hôtes
Hôte.Configuration.Connexion	Permet de modifier l'état de la connexion d'un hôte (connecté ou déconnecté).	Hôtes
Hôte.Configuration.Microprogramme	Permet de mettre à jour le microprogramme des hôtes ESXi.	Hôtes
Hôte.Configuration.Hyperthreading	Permet de mettre sous et hors tension la technologie Hyperthread dans un planificateur CPU d'hôte.	Hôtes
Hôte.Configuration.Configuration d'image	Permet de modifier l'image associée à un hôte.	
Hôte.Configuration.Maintenance	Permet de mettre l'hôte en mode maintenance et hors de ce mode, ainsi que d'arrêter et de redémarrer l'hôte.	Hôtes
Hôte.Configuration.Configuration de la mémoire	Permet de modifier la configuration de l'hôte.	Hôtes
Hôte.Configuration.Configuration réseau	Permet de configurer le réseau, le pare-feu et le réseau de vMotion.	Hôtes
Hôte.Configuration.Alimentation	Permet de configurer les paramètres de gestion de l'alimentation de l'hôte.	Hôtes
Hôte.Configuration.Interroger correctif	Permet de demander les correctifs installables et de les installer sur l'hôte.	Hôtes
Hôte.Configuration.Profil de sécurité et pare-feu	Permet de configurer les services Internet, tels que le protocole SSH, Telnet, SNMP et le pare-feu de l'hôte.	Hôtes
Hôte.Configuration.Configuration de la partition de stockage	Permet de gérer des partitions de la banque de données et de diagnostic de VMFS. Les utilisateurs disposant de ce privilège peuvent rechercher de nouveaux périphériques de stockage et gérer l'iSCSI.	Hôtes
Hôte.Configuration.Gestion du système	Permet à des extensions de manier le système de fichiers sur l'hôte.	Hôtes
Hôte.Configuration.Ressources système	Permet de mettre à jour la configuration de la hiérarchie des ressources système.	Hôtes
Hôte.Configuration.Configuration du démarrage automatique de machine virtuelle	Permet de modifier la commande de démarrage et d'arrêt automatique des machines virtuelles sur un hôte unique.	Hôtes

Inventaire d'hôte

Les privilèges d'inventaire d'hôte contrôlent l'ajout des hôtes à l'inventaire, l'ajout des hôtes aux clusters et le déplacement des hôtes dans l'inventaire.

Le tableau décrit les privilèges requis pour ajouter et déplacer des hôtes et des clusters dans l'inventaire.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-16. Privilèges d'inventaire d'hôte

Nom de privilège	Description	Requis sur
Hôte.Inventaire.Ajouter un hôte au cluster	Permet d'ajouter un hôte à un cluster existant.	Clusters
Hôte.Inventaire.Ajouter un hôte autonome	Permet d'ajouter un hôte autonome.	Dossiers d'hôte
Hôte.Inventaire.Créer cluster	Permet de créer un cluster.	Dossiers d'hôte
Hôte.Inventaire.Modifier cluster	Permet de changer les propriétés d'un cluster.	Clusters
Hôte.Inventaire.Déplacer un cluster ou un hôte autonome	Permet de déplacer un cluster ou un hôte autonome d'un dossier à l'autre. Le privilège doit être présent à la fois à la source et à la destination.	Clusters
Hôte.Inventaire.Déplacer un hôte	Permet de déplacer un ensemble d'hôtes existants au sein d'un cluster ou en dehors. Le privilège doit être présent à la fois à la source et à la destination.	Clusters
Hôte.Inventaire.Supprimer un cluster	Permet de supprimer un cluster ou un hôte autonome. Pour pouvoir exécuter cette opération, un utilisateur ou un groupe d'utilisateurs doit disposer de ce privilège attribué à la fois à l'objet et à son objet parent.	Clusters, hôtes
Hôte.Inventaire.Supprimer un hôte	Permet de supprimer un hôte. Pour pouvoir exécuter cette opération, un utilisateur ou un groupe d'utilisateurs doit disposer de ce privilège attribué à la fois à l'objet et à son objet parent.	Objet d'hôtes plus objet parent
Hôte.Inventaire.Renommer un cluster	Permet de renommer un cluster.	Clusters

Privilèges d'opérations locales d'hôte

Les privilèges d'opérations locales d'hôte contrôlent les actions effectuées lorsque VMware Host Client est connecté directement à un hôte.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-17. Privilèges d'opérations locales d'hôte

Nom de privilège	Description	Requis sur
Hôte.Opérations locales.Ajouter un hôte à vCenter	Permet d'installer et de supprimer des agents vCenter, tels que vpxa et aam, sur un hôte.	Hôte racine
Hôte.Opérations locales.Créer une machine virtuelle	Permet de créer une machine virtuelle entièrement nouvelle sur un disque sans l'enregistrer sur l'hôte.	Hôte racine
Hôte.Opérations locales.Supprimer une machine virtuelle	Permet de supprimer une machine virtuelle sur le disque. Cette opération est autorisée pour les machines virtuelles enregistrées comme pour celles dont l'enregistrement a été annulé.	Hôte racine

Tableau 10-17. Privilèges d'opérations locales d'hôte (suite)

Nom de privilège	Description	Requis sur
Hôte.Opérations locales.Gérer des groupes d'utilisateurs	Permet de gérer des comptes locaux sur un hôte.	Hôte racine
Hôte.Opérations locales.Reconfigurer une machine virtuelle	Permet de reconfigurer une machine virtuelle.	Hôte racine

Privilèges de réplication d'hôte vSphere

Les privilèges de vSphere Replication d'hôte contrôlent l'utilisation de la réplication de machine virtuelle par VMware vCenter Site Recovery Manager™ pour un hôte.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-18. Privilèges de réplication d'hôte vSphere

Nom de privilège	Description	Requis sur
Hôte.vSphere Replication.Gérer la réplication	Autorise la gestion de la réplication de machine virtuelle sur cet hôte.	Hôtes

Privilèges de profil d'hôte

Les privilèges de profil d'hôte contrôlent les opérations liées à la création et à la modification des profils d'hôte.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-19. Privilèges de profil d'hôte

Nom de privilège	Description	Requis sur
Profil d'hôte.Effacer	Permet d'effacer les informations liées au profil.	Instance racine de vCenter Server
Profil d'hôte.Créer	Permet la création d'un profil d'hôte.	Instance racine de vCenter Server
Profil d'hôte.Supprimer	Permet la suppression d'un profil d'hôte.	Instance racine de vCenter Server
Profil d'hôte.Modifier	Permet la modification d'un profil d'hôte.	Instance racine de vCenter Server
Profil d'hôte.Exporter	Permet l'exportation d'un profil d'hôte	Instance racine de vCenter Server
Profil d'hôte.Afficher	Permet l'affichage d'un profil d'hôte.	Instance racine de vCenter Server

Privilèges de réseau

Les privilèges de réseau contrôlent les tâches associées à la gestion du réseau.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-20. Privilèges de réseau

Nom de privilège	Description	Requis sur
Réseau.Attribuer un réseau	Permet l'attribution d'un réseau à une machine virtuelle.	Réseaux, machines virtuelles
Réseau.Configurer	Permet la configuration d'un réseau.	Réseaux, machines virtuelles
Réseau.Déplacer un réseau	Permet de déplacer un réseau entre des dossiers. Le privilège doit être présent à la fois à la source et à la destination.	Réseaux
Réseau.Supprimer	Permet la suppression d'un réseau. Ce privilège est à éviter. Pour pouvoir exécuter cette opération, un utilisateur ou un groupe d'utilisateurs doit disposer de ce privilège attribué à la fois à l'objet et à son objet parent.	Réseaux

Privilèges de performances

Les privilèges de performances contrôlent la modification de paramètres statistiques de performances.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-21. Privilèges de performances

Nom de privilège	Description	Requis sur
Performances.Modifier des intervalles	Permet la création, la suppression et la mise à jour d'intervalles de collecte de données de performance.	Instance racine de vCenter Server

Privilèges d'autorisations

Les privilèges d'autorisations contrôlent l'attribution des rôles et des autorisations.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-22. Privilèges d'autorisations

Nom de privilège	Description	Requis sur
Autorisations.Modifier une autorisation	Permet de définir une ou plusieurs règles d'autorisation sur une entité, ou met à jour des règles éventuellement déjà présentes, pour l'utilisateur ou le groupe donné de l'entité. Pour pouvoir exécuter cette opération, un utilisateur ou un groupe d'utilisateurs doit disposer de ce privilège attribué à la fois à l'objet et à son objet parent.	Tout objet plus objet parent
Autorisations.Modifier un privilège	Permet de modifier le groupe d'un privilège ou sa description. Aucun élément d'interface utilisateur de vSphere Web Client n'est associé à ce privilège.	
Autorisations.Modifier un rôle	Permet de mettre à jour du nom d'un rôle et des privilèges associés à ce rôle.	Tout objet
Autorisations.Réattribuer des autorisations de rôle	Permet la réattribution de toutes les autorisations d'un rôle à un autre rôle.	Tout objet

Privilèges de stockage basé sur le profil

Les privilèges de stockage basé sur le profil contrôlent les opérations liées aux profils de stockage.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-23. Privilèges de stockage basé sur le profil

Nom de privilège	Description	Requis sur
Stockage basé sur le profil.Mise à jour du stockage basé sur le profil	Permet d'apporter des modifications aux profils de stockage, telles que la création et la mise à jour de capacités de stockage et de profils de stockage de machine virtuelle.	Instance racine de vCenter Server
Stockage basé sur le profil.Vue du stockage basé sur le profil	Permet d'afficher les capacités de stockage et les profils de stockage définis.	Instance racine de vCenter Server

Privilèges de ressources

Les privilèges de ressource contrôlent la création et la gestion des pools de ressources, ainsi que la migration des machines virtuelles.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-24. Privilèges de ressources

Nom de privilège	Description	Requis sur
Ressource.Appliquer une recommandation	Permet d'accepter une suggestion du serveur pour effectuer une migration vers vMotion.	Clusters
Ressource.Attribuer un vApp au pool de ressources	Permet d'attribuer un vApp à un pool de ressources.	Pools de ressources
Ressource.Attribuer une machine virtuelle au pool de ressources	Permet d'attribuer une machine virtuelle à un pool de ressources.	Pools de ressources
Ressource.Créer un pool de ressources	Permet de créer un pool de ressources.	Pools de ressources, clusters
Ressource.Migrer une machine virtuelle hors tension	Permet de migrer une machine virtuelle hors tension vers un autre pool de ressources ou un autre hôte.	Machines virtuelles
Ressource.Migrer une machine virtuelle sous tension	Permet de migrer une machine virtuelle hors tension vers un autre pool de ressources ou un autre hôte à l'aide de vMotion.	
Ressource.Modifier un pool de ressources	Permet de changer les allocations d'un pool de ressources.	Pools de ressources
Ressource.Déplacer un pool de ressources	Permet de déplacer un pool de ressources. Le privilège doit être présent à la fois à la source et à la destination.	Pools de ressources
Ressource.Interroger vMotion	Permet d'interroger la compatibilité générale de la fonction vMotion d'une machine virtuelle avec un ensemble d'hôtes.	Instance racine de vCenter Server

Tableau 10-24. Privilèges de ressources (suite)

Nom de privilège	Description	Requis sur
Ressource.Supprimer un pool de ressources	Permet de supprimer un pool de ressources. Pour pouvoir exécuter cette opération, un utilisateur ou un groupe d'utilisateurs doit disposer de ce privilège attribué à la fois à l'objet et à son objet parent.	Pools de ressources
Ressource.Renommer un pool de ressources	Permet de renommer un pool de ressources.	Pools de ressources

Privilèges de tâche planifiée

Les privilèges de tâche planifiée contrôlent la création, l'édition et la suppression de tâches planifiées.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-25. Privilèges de tâche planifiée

Nom de privilège	Description	Requis sur
Tâche planifiée.Créer des tâches	Permet de planifier une tâche. Requis en plus des privilèges pour exécuter l'action programmée au moment de l'établissement de la planification.	Tout objet
Tâche planifiée.Modifier une tâche	Permet de reconfigurer les propriétés de tâche planifiée.	Tout objet
Tâche planifiée.Supprimer une tâche	Permet de supprimer une tâche planifiée de la file d'attente.	Tout objet
Tâche planifiée.Exécuter une tâche	Permet d'exécuter la tâche planifiée immédiatement. La création et l'exécution d'une tâche planifiée exigent également l'autorisation d'exécuter l'action associée.	Tout objet

Privilèges de sessions

Les privilèges de sessions contrôlent la capacité des extensions à ouvrir des sessions sur le système vCenter Server.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-26. Privilèges de session

Nom de privilège	Description	Requis sur
Sessions.Emprunter l'identité d'un utilisateur	Permet d'emprunter l'identité d'un autre utilisateur. Cette capacité est utilisée par des extensions.	Instance racine de vCenter Server
Sessions.Message	Permet de définir le message global de procédure de connexion.	Instance racine de vCenter Server
Sessions.Valider une session	Permet de vérifier la validité de la session.	Instance racine de vCenter Server
Sessions.Afficher et arrêter des sessions	Permet d'afficher les sessions et de forcer un ou plusieurs utilisateurs connectés à fermer leurs sessions.	Instance racine de vCenter Server

Privilèges de vues de stockage

Les privilèges pour les vues de stockage contrôlent les privilèges pour les API du service de surveillance du stockage. À partir de vSphere 6.0, les vues de stockage sont abandonnées et ces privilèges ne s'y appliquent plus.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-27. Privilèges de vues de stockage

Nom de privilège	Description	Requis sur
Vues de stockage.Configurer un service	Permet aux utilisateurs ayant des privilèges d'utiliser tous les API du service de surveillance du stockage. Utilisez **Vues de stockage.Afficher** pour les privilèges des API en lecture seule du service de surveillance du stockage.	Instance racine de vCenter Server
Vues de stockage.Afficher	Permet aux utilisateurs ayant des privilèges d'utiliser les API en lecture seule du service de surveillance du stockage.	Instance racine de vCenter Server

Privilèges de tâches

Les privilèges de tâches contrôlent la capacité des extensions à créer et mettre à jour des tâches sur vCenter Server.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-28. Privilèges de tâches

Nom de privilège	Description	Requis sur
Tâches.Créer une tâche	Permet à une extension de créer une tâche définie par l'utilisateur. Aucun élément d'interface utilisateur de vSphere Web Client n'est associé à ce privilège.	Instance racine de vCenter Server
Tâches.Mettre à jour une tâche	Permet à une extension de mettre à niveau une tâche définie par l'utilisateur. Aucun élément d'interface utilisateur de vSphere Web Client n'est associé à ce privilège.	Instance racine de vCenter Server

Privilèges Transfer Service

Les privilèges Transfer Service sont internes à VMware. N'utilisez pas ces privilèges.

Privilèges de configuration de machine virtuelle

Les privilèges de configuration de la machine virtuelle contrôlent la capacité de configuration des options et des périphériques de machine virtuelle.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-29. Privilèges de configuration de machine virtuelle

Nom de privilège	Description	Requis sur
Machine virtuelle.Configuration.Ajouter un disque existant	Permet l'ajout d'un disque virtuel existant à une machine virtuelle.	Machines virtuelles
Machine virtuelle.Configuration.Ajouter un nouveau disque	Permet la création d'un disque virtuel à ajouter à une machine virtuelle.	Machines virtuelles
Machine virtuelle.Configuration.Ajouter ou supprimer un périphérique	Permet l'ajout ou la suppression de n'importe quel périphérique non-disque.	Machines virtuelles
Machine virtuelle.Configuration.Avancé	Permet l'ajout ou la modification de paramètres avancés dans le fichier de configuration de la machine virtuelle.	Machines virtuelles
Machine virtuelle.Configuration.Modifier le nombre de CPU	Permet de changer le nombre de CPU virtuels.	Machines virtuelles
Machine virtuelle.Configuration.Changer une ressource	Permet la modification de la configuration des ressources d'un ensemble de nœuds de machine virtuelle dans un pool de ressources donné.	Machines virtuelles
Machine virtuelle.Configuration.Configurer managedBy	Permet à une extension ou à une solution de marquer une machine virtuelle comme étant gérée par cette extension ou solution.	Machines virtuelles
Machine virtuelle.Configuration.Suivi des changements de disques	Permet l'activation ou la désactivation du suivi des modifications des disques de la machine virtuelle.	Machines virtuelles
Machine virtuelle.Configuration.Bail de disque	Permet des opérations de bail de disque pour une machine virtuelle.	Machines virtuelles
Machine virtuelle.Configuration.Afficher les paramètres de connexion	Permet de configurer les options de la console distante d'une machine virtuelle.	Machines virtuelles
Machine virtuelle.Configuration.Développer un disque virtuel	Permet d'étendre la taille d'un disque virtuel.	Machines virtuelles
Machine virtuelle.Configuration.Périphérique USB hôte	Permet d'attacher à une machine virtuelle un périphérique USB hébergé sur hôte.	Machines virtuelles

Tableau 10-29. Privilèges de configuration de machine virtuelle (suite)

Nom de privilège	Description	Requis sur
Machine virtuelle.Configuration.Mémoire	Permet de changer la quantité de mémoire allouée à la machine virtuelle.	Machines virtuelles
Machine virtuelle.Configuration.Modifier les paramètres de périphérique	Permet de changer les propriétés d'un périphérique existant.	Machines virtuelles
Machine virtuelle.Configuration.Interroger la compatibilité avec Fault Tolerance	Permet de contrôler si une machine virtuelle est compatible avec Fault Tolerance.	Machines virtuelles
Machine virtuelle.Configuration.Interroger des fichiers sans propriétaire	Permet d'interroger des fichiers sans propriétaire.	Machines virtuelles
Machine virtuelle.Configuration.Périphérique brut	Permet d'ajouter ou de retirer un mappage de disque brut ou un périphérique de relais SCSI. La définition de ce paramètre ne tient compte d'aucun autre privilège pour modifier les périphériques bruts, y compris des états de connexion.	Machines virtuelles
Machine virtuelle.Configuration.Recharger à partir du chemin d'accès	Permet de changer un chemin de configuration de machine virtuelle tout en préservant l'identité de la machine virtuelle. Les solutions telles que VMware vCenter Site Recovery Manager utilisent cette opération pour préserver l'identité de la machine virtuelle pendant le basculement et la restauration automatique.	Machines virtuelles
Machine virtuelle.Configuration.Supprimer un disque	Permet la suppression d'un périphérique de disque virtuel.	Machines virtuelles
Machine virtuelle.Configuration.Renommer	Permet de renommer une machine virtuelle ou de modifier les notes associées d'une machine virtuelle.	Machines virtuelles
Machine virtuelle.Configuration.Réinitialiser des informations d'invité	Permet de modifier les informations du système d'exploitation invité d'une machine virtuelle	Machines virtuelles
Machine virtuelle.Configuration.Définir une annotation	Permet d'ajouter ou de modifier une annotation de machine virtuelle.	Machines virtuelles
Machine virtuelle.Configuration.Paramètres	Permet de modifier les paramètres généraux d'une machine virtuelle.	Machines virtuelles
Machine virtuelle.Configuration.Emplacement du fichier d'échange	Permet de changer la règle de placement du fichier d'échange d'une machine virtuelle.	Machines virtuelles
Machine virtuelle.Configuration.Activer/Désactiver le parent de déviation		
Machine virtuelle.Configuration.Mettre à niveau la compatibilité de machine virtuelle	Permet la mise à niveau de la version de compatibilité des machines virtuelles.	Machines virtuelles

Privilèges d'opérations d'invité de machine virtuelle

Les privilèges d'opérations d'invité de machine virtuelle contrôlent la capacité à interagir avec les fichiers et les programmes au sein du système d'exploitation invité d'une machine virtuelle avec l'API.

Pour obtenir plus d'informations sur ces opérations, consultez la documentation *Référence de VMware vSphere API*.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-30. Opérations de système invité d'une machine virtuelle

Nom de privilège	Description	Pertinent sur l'objet
Machine virtuelle.Systèmes invités.Modification d'alias d'un système invité	Autorise les opérations d'invité d'une machine virtuelle impliquant la modification de l'alias de la machine virtuelle.	Machines virtuelles
Machine virtuelle.Systèmes invités.Requête d'alias d'un système invité	Autorise les opérations d'invité d'une machine virtuelle impliquant l'interrogation de l'alias de la machine virtuelle.	Machines virtuelles
Machine virtuelle.Systèmes invités.Modifications d'un système invité	Autorise les opérations de système invité d'une machine virtuelle impliquant des modifications apportées au système d'exploitation invité d'une machine virtuelle, telles que le transfert d'un fichier vers la machine virtuelle. Aucun élément d'interface utilisateur de vSphere Web Client n'est associé à ce privilège.	Machines virtuelles
Machine virtuelle.Systèmes invités.Exécution du programme d'un système invité	Autorise les opérations de système invité d'une machine virtuelle impliquant l'exécution d'un programme dans la machine virtuelle. Aucun élément d'interface utilisateur de vSphere Web Client n'est associé à ce privilège.	Machines virtuelles
Machine virtuelle.Systèmes invités.Requêtes d'un système invité	Autorise les opérations de système invité d'une machine virtuelle impliquant l'interrogation du système d'exploitation invité, telles que l'énumération des fichiers du système d'exploitation invité. Aucun élément d'interface utilisateur de vSphere Web Client n'est associé à ce privilège.	Machines virtuelles

Privilèges d'interaction de machine virtuelle

Les privilèges d'interaction de machine virtuelle contrôlent la capacité à interagir avec une console de machine virtuelle, à configurer des médias, à exécuter des opérations d'alimentation et à installer VMware Tools.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-31. Interaction de machine virtuelle

Nom de privilège	Description	Requis sur
Machine virtuelle.Interaction .Répondre à une question	Permet de résoudre les problèmes de transitions d'état ou d'erreurs d'exécution de la machine virtuelle.	Machines virtuelles
Machine virtuelle.Interaction .Opération de sauvegarde sur machine virtuelle	Permet d'exécuter des opérations de sauvegarde sur des machines virtuelles.	Machines virtuelles
Machine virtuelle .Interaction .Configurer un support sur CD	Permet de configurer un DVD virtuel ou un lecteur de CD-ROM.	Machines virtuelles

Tableau 10-31. Interaction de machine virtuelle (suite)

Nom de privilège	Description	Requis sur
Machine virtuelle .Interaction .Configurer un support sur disquette	Permet de configurer un périphérique de disquettes virtuel.	Machines virtuelles
Machine virtuelle .Interaction .Interaction avec une console	Permet d'interagir avec la souris virtuelle, le clavier et l'écran de la machine virtuelle.	Machines virtuelles
Machine virtuelle .Interaction .Créer une capture d'écran	Permet de créer une capture d'écran de machine virtuelle.	Machines virtuelles
Machine virtuelle .Interaction .Défragmenter tous les disques	Permet de défragmenter des opérations sur tous les disques sur la machine virtuelle.	Machines virtuelles

Tableau 10-31. Interaction de machine virtuelle (suite)

Nom de privilège	Description	Requis sur
Machine virtuelle .Interaction .Connexion à un périphérique	Permet de modifier l'état connecté des périphériques virtuels déconnectables d'une machine virtuelle.	Machines virtuelles
Machine virtuelle .Interaction .Glisser-déplacer	Permet le glisser-déplacer de fichiers entre une machine virtuelle et un client distant.	Machines virtuelles
Machine virtuelle .Interaction .Gestion par VIX API d'un système d'exploitation invité	Permet de gérer le système d'exploitation de la machine virtuelle via VIX API.	Machines virtuelles
Machine virtuelle .Interaction .Injecter des codes de balayage HID USB	Permet l'injection de codes de balayage HID USB.	Machines virtuelles

Tableau 10-31. Interaction de machine virtuelle (suite)

Nom de privilège	Description	Requis sur
Machine virtuelle .Interaction .Interrompre ou reprendre	Permet l'interruption ou la reprise de la machine virtuelle.	Machines virtuelles
Machine virtuelle .Interaction .Exécuter des opérations d'effacement ou de réduction	Permet d'effectuer des opérations d'effacement ou de réduction sur la machine virtuelle.	Machines virtuelles
Machine virtuelle .Interaction .Mettre hors tension	Permet de mettre hors tension une machine virtuelle sous tension. Cette opération met hors tension le système d'exploitation invité.	Machines virtuelles

Tableau 10-31. Interaction de machine virtuelle (suite)

Nom de privilège	Description	Requis sur
Machine virtuelle .Interaction .Mettre sous tension	Permet de mettre sous tension une machine virtuelle hors tension et de redémarrer une machine virtuelle interrompue.	Machines virtuelles
Machine virtuelle .Interaction .Session d'enregistrement sur machine virtuelle	Permet d'enregistrer une session sur une machine virtuelle.	Machines virtuelles
Machine virtuelle .Interaction .Session de relecture sur machine virtuelle	Permet de réinsérer une session enregistrée sur une machine virtuelle.	Machines virtuelles
Machine virtuelle .Interaction .Réinitialiser	Permet de réinitialiser une machine virtuelle et redémarre le système d'exploitation invité.	Machines virtuelles

Tableau 10-31. Interaction de machine virtuelle (suite)

Nom de privilège	Description	Requis sur
Machine virtuelle .Interaction .Relancer Fault Tolerance	Permet la reprise de Fault Tolerance pour une machine virtuelle.	Machines virtuelles
Machine virtuelle .Interaction .Interrompre	Permet d'interrompre une machine virtuelle sous tension. Cette opération met l'invité en mode veille.	Machines virtuelles
Machine virtuelle .Interaction .Interrompre Fault Tolerance	Permet la suspension de Fault Tolerance pour une machine virtuelle.	Machines virtuelles

Tableau 10-31. Interaction de machine virtuelle (suite)

Nom de privilège	Description	Requis sur
Machine virtuelle .Interaction .Tester le basculement	Permet de tester le basculement de Fault Tolerance en faisant de la machine virtuelle secondaire la machine virtuelle principale.	Machines virtuelles
Machine virtuelle .Interaction .Tester le redémarrage de la VM secondaire	Permet de terminer une machine virtuelle secondaire pour une machine virtuelle utilisant Fault Tolerance.	Machines virtuelles
Machine virtuelle .Interaction .Désactiver Fault Tolerance	Permet de mettre hors tension Fault Tolerance pour une machine virtuelle.	Machines virtuelles

Tableau 10-31. Interaction de machine virtuelle (suite)

Nom de privilège	Description	Requis sur
Machine virtuelle .Interaction .Activer Fault Tolerance	Permet de mettre sous tension Fault Tolerance pour une machine virtuelle.	Machines virtuelles
Machine virtuelle .Interaction .Installation de VMware Tools	Permet de monter et démonter le programme d'installation CD de VMware Tools comme un CD-ROM pour le système d'exploitation invité.	Machines virtuelles

Privilèges d'inventaire de machine virtuelle

Les privilèges d'inventaire de machine virtuelle contrôlent l'ajout, le déplacement et la suppression des machines virtuelles.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-32. Privilèges d'inventaire de machine virtuelle

Nom de privilège	Description	Requis sur
Machine virtuelle .Inventaire.Créer à partir d'un modèle existant	Permet la création d'une machine virtuelle basée sur une machine virtuelle existante ou un modèle existant, par clonage ou déploiement à partir d'un modèle.	Clusters, hôtes, dossiers de machine virtuelle
Machine virtuelle .Inventaire.Créer	Permet la création d'une machine virtuelle et l'allocation de ressources pour son exécution.	Clusters, hôtes, dossiers de machine virtuelle
Machine virtuelle .Inventaire.Déplacer	Permet le déplacement d'une machine virtuelle dans la hiérarchie. Le privilège doit être présent à la fois à la source et à la destination.	Machines virtuelles

Tableau 10-32. Privilèges d'inventaire de machine virtuelle (suite)

Nom de privilège	Description	Requis sur
Machine virtuelle .Inventaire.Enregistrer	Permet d'ajouter une machine virtuelle existante à vCenter Server ou à un inventaire d'hôtes.	Clusters, hôtes, dossiers de machine virtuelle
Machine virtuelle .Inventaire.Supprimer	Permet la suppression d'une machine virtuelle. L'opération supprime du disque les fichiers sous-jacents de la machine virtuelle. Pour pouvoir exécuter cette opération, un utilisateur ou un groupe d'utilisateurs doit disposer de ce privilège attribué à la fois à l'objet et à son objet parent.	Machines virtuelles
Machine virtuelle .Inventaire.Annuler l'enregistrement	Permet l'annulation de l'enregistrement d'une machine virtuelle d'une instance de vCenter Server ou d'un inventaire d'hôte. Pour pouvoir exécuter cette opération, un utilisateur ou un groupe d'utilisateurs doit disposer de ce privilège attribué à la fois à l'objet et à son objet parent.	Machines virtuelles

Privilèges de provisionnement de machine virtuelle

Les privilèges de provisionnement de machine virtuelle contrôlent les activités associées au déploiement et à la personnalisation des machines virtuelles.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-33. Privilèges de provisionnement de machine virtuelle

Nom de privilège	Description	Requis sur
Machine virtuelle .Provisionnement.Autoriser l'accès au disque	Permet d'ouvrir un disque sur une machine virtuelle pour l'accès aléatoire en lecture et en écriture. Utilisé en majeure partie pour le montage distant de disque.	Machines virtuelles
Machine virtuelle .Provisionnement.Autoriser l'accès au fichier	Permet d'effectuer des opérations sur des fichiers associés à une machine virtuelle, y compris les fichiers vmx, les disques, les journaux et les nvram.	Machines virtuelles
Machine virtuelle .Provisionnement.Autoriser l'accès au disque en lecture seule	Permet d'ouvrir un disque sur une machine virtuelle pour l'accès aléatoire en lecture. Utilisé en majeure partie pour le montage distant de disque.	Machines virtuelles
Machine virtuelle .Provisionnement.Autoriser le téléchargement de machines virtuelles	Permet de lire des fichiers associés à une machine virtuelle, y compris les fichiers vmx, les disques, les journaux et les nvram.	Hôte racine ou instance racine de vCenter Server
Machine virtuelle .Provisionnement.Autoriser le téléchargement de fichiers de machine virtuelle	Permet d'écrire sur des fichiers associés à une machine virtuelle, y compris les fichiers vmx, les disques, les journaux et les nvram.	Hôte racine ou instance racine de vCenter Server
Machine virtuelle .Provisionnement.Cloner un modèle	Permet de cloner un modèle.	Modèles
Machine virtuelle .Provisionnement.Cloner une machine virtuelle	Permet de cloner une machine virtuelle existante et d'allouer des ressources.	Machines virtuelles

Tableau 10-33. Privilèges de provisionnement de machine virtuelle (suite)

Nom de privilège	Description	Requis sur
Machine virtuelle .Provisionnement.Créer un modèle à partir d'une machine virtuelle	Permet de créer un nouveau modèle à partir d'une machine virtuelle.	Machines virtuelles
Machine virtuelle .Provisionnement.Personnaliser	Permet de personnaliser le système d'exploitation invité d'une machine virtuelle sans déplacer cette dernière.	Machines virtuelles
Machine virtuelle .Provisionnement.Déployer un modèle	Permet de déployer une machine virtuelle à partir d'un modèle.	Modèles
Machine virtuelle .Provisionnement. Marquer comme modèle	Permet de marquer une machine virtuelle existante hors tension comme modèle.	Machines virtuelles
Machine virtuelle .Provisionnement. Marquer comme machine virtuelle	Permet de marquer un modèle existant comme machine virtuelle.	Modèles
Machine virtuelle .Provisionnement. Modifier la spécification de personnalisation	Permet de créer, modifier ou supprimer des spécifications de personnalisation.	Instance racine de vCenter Server
Machine virtuelle .Provisionnement.Promouvoir des disques	Permet de promouvoir des opérations sur les disques d'une machine virtuelle.	Machines virtuelles
Machine virtuelle .Provisionnement.Lire les spécifications de personnalisation	Permet de lire une spécification de personnalisation.	Machines virtuelles

Privilèges de configuration de services de machine virtuelle

Les privilèges de configuration de services de machine virtuelle contrôlent qui peut exécuter une tâche de surveillance de gestion sur la configuration des services.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Remarque Dans vSphere 6.0, n'attribuez pas et ne supprimez pas ce privilège à l'aide de vSphere Web Client.

Tableau 10-34. Privilèges de configuration de services de machine virtuelle

Nom de privilège	Description
Machine virtuelle. Configuration de service. Autoriser les notifications	Permet la génération et la consommation de notifications sur l'état des services.
Machine virtuelle. Configuration de service. Autoriser l'interrogation des notifications d'événements globales	Permet de déterminer la présence éventuelle de notifications.
Machine virtuelle. Configuration de service. Gérer les configurations de service	Permet la création, la modification et la suppression de services de machine virtuelle.

Tableau 10-34. Privilèges de configuration de services de machine virtuelle (suite)

Nom de privilège	Description
Machine virtuelle. Configuration de service. Modifier une configuration de service	Permet la modification d'une configuration de services d'une machine virtuelle existante.
Machine virtuelle. Configuration de service. Interroger les configurations de service	Permet la récupération d'une liste de services de machine virtuelle.
Machine virtuelle. Configuration de service. Lire une configuration de service	Permet la récupération d'une configuration de services d'une machine virtuelle existante.

Privilèges de gestion des snapshots d'une machine virtuelle

Les privilèges de gestion des snapshots d'une machine virtuelle contrôlent la capacité à prendre, supprimer, renommer et restaurer des snapshots.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-35. Privilèges d'état de machine virtuelle

Nom de privilège	Description	Requis sur
Machine virtuelle .Gestion des snapshots. Créer un snapshot	Permet de créer un nouveau snapshot de l'état actuel de la machine virtuelle.	Machines virtuelles
Machine virtuelle .Gestion des snapshots.Supprimer un snapshot	Permet de supprimer un snapshot de l'historique de snapshots.	Machines virtuelles
Machine virtuelle .Gestion des snapshots.Renommer un snapshot	Permet de renommer un snapshot avec un nouveau nom, une nouvelle description, ou les deux.	Machines virtuelles
Machine virtuelle .Gestion des snapshots.Restaurer un snapshot	Permet de paramétrer la machine virtuelle à l'état où elle était à un snapshot donné.	Machines virtuelles

Privilèges vSphere Replication de machine virtuelle

Les privilèges vSphere Replication de machine virtuelle contrôlent l'utilisation de la réplication par VMware vCenter Site Recovery Manager™ pour les machines virtuelles.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-36. Réplication de machine virtuelle vSphere

Nom de privilège	Description	Requis sur
Machine virtuelle .vSphere Replication.Configurer la réplication	Permet de configurer la réplication de la machine virtuelle.	Machines virtuelles
Machine virtuelle .vSphere Replication.Gérer la réplication	Permet de déclencher la synchronisation complète, la synchronisation en ligne ou la synchronisation hors ligne d'une réplication.	Machines virtuelles
Machine virtuelle .vSphere Replication.Surveiller la réplication	Permet de contrôler la réplication.	Machines virtuelles

Privilèges du groupe dvPort

Les privilèges de groupes de ports virtuels distribués contrôlent la capacité à créer, supprimer et modifier les groupes de ports virtuels distribués.

Le tableau décrit les privilèges requis pour créer et configurer des groupes de ports virtuels distribués.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-37. Privilèges de groupes de ports virtuels distribués

Nom de privilège	Description	Requis sur
Groupe dvPort.Créer	Permet de créer un groupe de ports virtuels distribués.	Groupes de ports virtuels
Groupe dvPort.Supprimer	Permet de supprimer un groupe de ports virtuels distribués. Pour pouvoir exécuter cette opération, un utilisateur ou un groupe d'utilisateurs doit disposer de ce privilège attribué à la fois à l'objet et à son objet parent.	Groupes de ports virtuels
Groupe dvPort.Modifier	Permet de modifier la configuration d'un groupe de ports virtuels distribués.	Groupes de ports virtuels
Groupe dvPort.Opération de stratégie	Permet de définir la règle d'un groupe de ports virtuels distribués.	Groupes de ports virtuels
Groupe dvPort.Opération de portée	Permet de définir la portée d'un groupe de ports virtuels distribués.	Groupes de ports virtuels

Privilèges de vApp

Les privilèges vApp contrôlent des opérations associées au déploiement et à la configuration d'un vApp.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-38. Privilèges de vApp

Nom de privilège	Description	Requis sur
vApp.Ajouter une machine virtuelle	Permet d'ajouter une machine virtuelle à un vApp.	vApps
vApp.Attribuer un pool de ressources	Permet d'attribuer un pool de ressources à un vApp.	vApps
vApp.Attribuer un vApp	Permet d'attribuer un vApp à un autre vApp.	vApps
vApp.Cloner	Permet de cloner un vApp.	vApps
vApp.Créer	Permet de créer un vApp.	vApps
vApp.Supprimer	Permet de supprimer un vApp. Pour pouvoir exécuter cette opération, un utilisateur ou un groupe d'utilisateurs doit disposer de ce privilège attribué à la fois à l'objet et à son objet parent.	vApps
vApp.Exporter	Permet d'exporter un vApp à partir de vSphere.	vApps
vApp.Importer	Permet d'importer un vApp dans vSphere.	vApps
vApp.Déplacer	Permet de déplacer un vApp vers un nouvel emplacement d'inventaire.	vApps
vApp.Mettre hors tension	Permet de désactiver des opérations sur un vApp.	vApps
vApp.Mettre sous tension	Permet d'activer des opérations sur un vApp.	vApps
vApp.Renommer	Permet de renommer un vApp.	vApps
vApp.Interrompre	Permet d'interrompre un vApp.	vApps
vApp.Annuler un enregistrement	Permet d'annuler l'enregistrement d'un vApp. Pour pouvoir exécuter cette opération, un utilisateur ou un groupe d'utilisateurs doit disposer de ce privilège attribué à la fois à l'objet et à son objet parent.	vApps
vApp.Afficher l'environnement OVF	Permet de consulter l'environnement OVF d'une machine virtuelle sous tension au sein d'un vApp.	vApps
vApp.Configuration d'une application de vApp	Permet de modifier la structure interne d'un vApp, telle que l'information produit et les propriétés.	vApps
vApp.Configuration d'une instance de vApp	Permet de modifier la configuration d'une instance de vApp, telle que les stratégies.	vApps
vApp.Configuration de vApp managedBy	Permet à une extension ou à une solution de marquer un vApp comme étant géré par cette extension ou solution. Aucun élément d'interface utilisateur de vSphere Web Client n'est associé à ce privilège.	vApps
vApp.Configuration des ressources de vApp	Permet de modifier la configuration des ressources d'un vApp. Pour pouvoir exécuter cette opération, un utilisateur ou un groupe d'utilisateurs doit disposer de ce privilège attribué à la fois à l'objet et à son objet parent.	vApps

Privilèges vServices

Les privilèges vServices contrôlent la capacité à créer, configurer et mettre à niveau les dépendances vService des machines virtuelles et des vApp.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-39. vServices

Nom de privilège	Description	Requis sur
vService.Créer une dépendance	Permet de créer une dépendance vService pour une machine virtuelle ou un vApp.	vApp et machines virtuelles
vService.Détruire la dépendance	Permet de supprimer une dépendance vService d'une machine virtuelle ou d'un vApp.	vApp et machines virtuelles
vService.Reconfigurer la configuration de dépendance	Permet la reconfiguration d'une dépendance pour mettre à jour le fournisseur ou la liaison.	vApp et machines virtuelles
vService.Mettre à jour la dépendance	Permet des mises à jour d'une dépendance pour configurer le nom ou la description.	vApp et machines virtuelles

Privilèges de balisage vSphere

Les privilèges de balisage vSphere contrôlent la capacité à créer et supprimer des balises et des catégories de balises, ainsi qu'à attribuer et supprimer des balises sur les objets d'inventaire vCenter Server.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 10-40. Privilèges de balisage vSphere

Nom de privilège	Description	Requis sur
Balisage vSphere.Attribuer une balise vSphere ou en annuler l'attribution	Permet d'attribuer ou non une balise pour un objet dans l'inventaire vCenter Server.	Tout objet
Balisage vSphere.Créer une balise vSphere	Permet de créer une balise.	Tout objet
Balisage vSphere.Créer une catégorie de balises vSphere	Permet de créer une catégorie de balise.	Tout objet
Balisage vSphere.Créer une étendue de balises vSphere	Permet la création d'une étendue de balise.	Tout objet
Balisage vSphere.Supprimer une balise vSphere	Permet de supprimer une catégorie de balise.	Tout objet
Balisage vSphere.Supprimer une catégorie de balises vSphere	Permet de supprimer une catégorie de balise.	Tout objet
Balisage vSphere.Supprimer une étendue de balises vSphere	Permet la suppression d'une étendue de balise.	Tout objet
Balisage vSphere.Modifier une balise vSphere	Permet de modifier une balise.	Tout objet
Balisage vSphere.Modifier une catégorie de balises vSphere	Permet la modification d'une catégorie de balise.	Tout objet

Tableau 10-40. Privilèges de balisage vSphere (suite)

Nom de privilège	Description	Requis sur
Balisage vSphere.Modifier une étendue de balises vSphere	Permet la modification d'une étendue de balise.	Tout objet
Balisage vSphere.Modifier le champ Utilisé par d'une catégorie	Permet la modification du champ UsedBy pour une catégorie de balise.	Tout objet
Balisage vSphere.Modifier le champ Utilisé par d'une balise	Permet la modification du champ UsedBy pour une balise.	Tout objet

Index

D

E

N

O

P

Q

R

S

T