Sécurité vSphere

ESXi 5.0

vCenter Serveur 5.0

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-000590-00

vmware®

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

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

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 ce guide

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

Pour vous permettre de protéger votre installation ESXi™ , cette documentation décrit les fonctions de sécurité intégrées à ESXi et les mesures que vous pouvez prendre pour la protéger des attaques.

Public cible

Ces informations s'adressent à toutes les personnes désirant protéger leur configuration ESXi. Elles sont destinées aux administrateurs Windows ou Linux expérimentés qui maîtrisent les technologies de machine virtuelle et les opérations de centre de données.

Sécurité pour systèmes ESXi 1

ESXi est développé avec une priorité de sécurité renforcée. VMware garantit la sécurité de l'environnement ESXi et entoure l'architecture système d'un niveau élevé de sécurité.

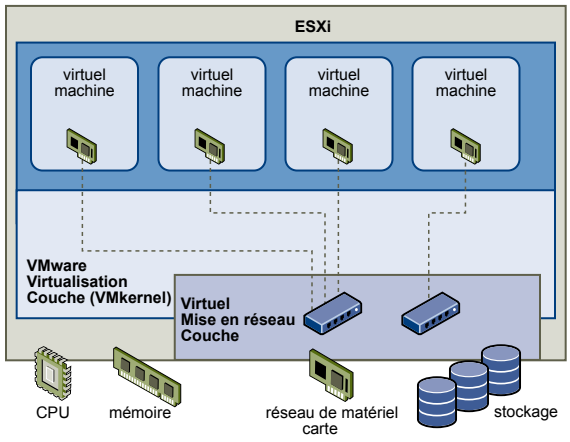
Ce chapitre aborde les rubriques suivantes :

Architecture ESXi et fonctions de sécurité

Les composants et l'architecture globale d'ESXi sont conçus pour garantir la sécurité du système ESXi entier.

Sous l'angle de la sécurité, ESXi contient trois composants principaux : la couche de virtualisation, les machines virtuelles et la couche réseau virtuelle.

Figure 1-1. Architecture ESXi



Sécurité et couche de virtualisation

VMware a conçu la couche de virtualisation (appelée VMkernel) pour l'exécution des machines virtuelles. Cette couche contrôle les composants matériels que les hôtes utilisent et planifie l'allocation des ressources matérielles sur les différentes machines virtuelles. VMkernel est totalement dédié à l'exécution des machines virtuelles et n'est pas utilisé pour d'autres fonctions. Par conséquent, son interface est strictement limitée à l'API requise pour la gestion des machines virtuelles.

ESXi offre une protection VMkernel supplémentaire pour les fonctions suivantes :

Durcissement de la mémoire

Le noyau ESXi, les applications utilisateur et les composants exécutables (pilotes et bibliothèques, par exemple) se trouvent à des emplacements mémoire aléatoires, non prévisibles. Cette fonction, associée aux protections mémoire des microprocesseurs, rend plus difficile l'utilisation de la mémoire par un code malveillant à des fins d'exploitation des vulnérabilités.

Intégrité du module noyau

Grâce à la signature numérique, l'intégrité et l'authenticité des modules, pilotes et applications sont les mêmes que si ces éléments étaient chargés par VMkernel. Cette signature permet à ESXi d'identifier les fournisseurs des modules, pilotes ou applications concernés, et de vérifier s'ils sont dotés d'une certification VMware.

TPM (Trusted Platform Module)

Ce module est un élément matériel qui représente le cœur d'une plate-forme matérielle, et qui permet d'obtenir l'attestation de processus de démarrage, de stockage de clés cryptographique et de protection. A chaque démarrage d'ESXi, TPM mesure la valeur VMkernel utilisée par ESXi et la consigne dans l'un des registres PCR (Platform Configuration Register). Les mesures TPM sont ensuite communiquées à vCenter Server, au moment où l'hôte est ajouté au système vCenter Server.

Vous pouvez utiliser TPM avec des solutions tierces pour fournir à l'image ESXi une protection basée sur la stratégie contre les menaces suivantes :

- Corruption de l'image stockée
- Certaines sortes de sabotage
- Mises à jour non prévues ou non autorisées et autres types de modifications

Activez le lancement dynamique de VMkernel à l'aide de TPM, grâce à l'option de configuration avancée `enableTboot` de vSphere Client. Elle porte le nom de Dynamic Root of Trust for Measurement (DRTM). Par défaut, l'utilisation de DRTM pour la mesure de VMkernel est désactivée.

Remarque Si le module TPM est présent sur un système mais désactivé dans le BIOS, le message d'erreur suivant est susceptible de s'afficher : `Error loading TPM` (erreur lors du chargement de TPM). Il s'agit d'un comportement normal ; vous pouvez ignorer ce message d'erreur.

Sécurité et machines virtuelles

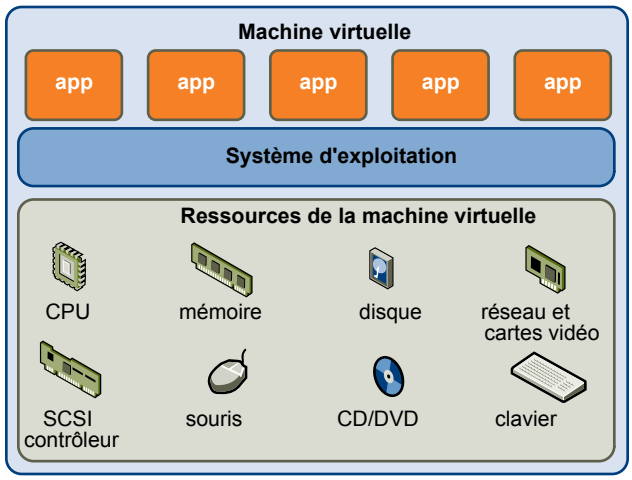
Les machines virtuelles sont les conteneurs dans lesquels sont exécutés les systèmes d'exploitation invités et les applications. Dès la conception, toutes les machines virtuelles VMware sont isolées les unes des autres. Cette isolation permet l'exécution en toute sécurité de plusieurs machines virtuelles malgré le partage de composants matériels. Ces machines affichent à la fois une bonne capacité d'accès aux composants matériels et des performances ininterrompues.

Même si un utilisateur possède des privilèges d'administrateur d'accès au système d'exploitation invité d'une machine virtuelle, il ne peut pas contourner cette couche d'isolation pour accéder à une autre machine virtuelle sans posséder les privilèges explicitement accordées par l'administrateur système ESXi. Avec l'isolation des machines virtuelles, en cas de défaillance d'un système d'exploitation invité, les autres machines virtuelles de l'hôte continuent de fonctionner. La panne du système d'exploitation invité n'affecte pas :

- La capacité des utilisateurs à accéder aux autres machines virtuelles
- La capacité des machines virtuelles opérationnelles à accéder aux ressources dont elles ont besoin
- Les performances des autres machines virtuelles

Chaque machine virtuelle est isolée des autres machines virtuelles exécutées sur le même équipement. Bien que les machines virtuelles partagent des ressources physiques (unité centrale, mémoire ou dispositifs d'E/S, par exemple), un système d'exploitation invité de machine virtuelle individuelle ne peut détecter aucun périphérique autre que les périphériques virtuels mis à sa disposition.

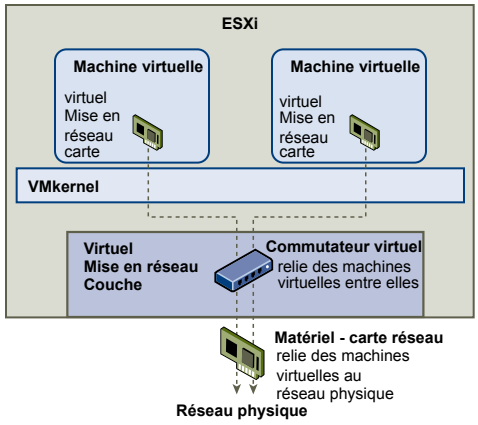
Figure 1-2. Isolation des machines virtuelles



VMkernel s'interpose entre les ressources physiques ; par ailleurs, tous les accès aux composants matériels s'effectuent via VMkernel ; les machines virtuelles ne peuvent donc pas contourner ce niveau d'isolation.

Une machine physique communique avec les autres machines d'un réseau via l'utilisation d'un adaptateur réseau. De la même façon, une machine virtuelle communique avec les autres machines virtuelles du même hôte via un commutateur virtuel. Une machine virtuelle communique également avec le réseau physique (y compris avec les machines virtuelles situées sur d'autres hôtes ESXi) via un adaptateur réseau physique.

Figure 1-3. Mise en réseau virtuel via l'utilisation de commutateurs virtuels



Les caractéristiques suivantes s'appliquent à l'isolation de machines virtuelles au sein d'un contexte réseau :

- Si une machine virtuelle ne partage pas de commutateur virtuel avec une autre machine virtuelle, elle est totalement isolée des réseaux virtuels de l'hôte.
- Si aucun adaptateur réseau physique n'est configurée pour une machine virtuelle, celle-ci est totalement isolée des réseaux physiques.
- Si vous utilisez les mêmes mesures de sécurité (pare-feu, logiciel anti-virus, notamment) pour assurer la protection d'une machine virtuelle d'un réseau que celles destinées à protéger une machine physique, la machine virtuelle bénéficie du même niveau de sécurité que la machine physique.

Vous pouvez renforcer la protection des machines virtuelles via la configuration de réservations de ressources et de limites sur l'hôte. Par exemple, grâce aux contrôles de ressources détaillés disponibles dans ESXi, vous pouvez configurer une machine virtuelle afin qu'elle puisse systématiquement recevoir 10 % minimum des ressources en unité centrale de l'hôte, mais sans jamais excéder 20 %.

Les réservations et limites de ressources protègent les machines virtuelles contre toute diminution de performances résultant de la consommation excessive, par une autre machine virtuelle, des ressources matérielles partagées. Par exemple, si l'une des machines virtuelles d'un hôte subit une attaque de déni de service (DoS), la limite de ressource appliquée à cette machine évite que les autres machines virtuelles ne soient affectées par la capture d'une quantité importante de ressources matérielles. De la même façon, la réservation de ressources appliquée à chaque machine virtuelle permet, en cas de forte demande de ressources émanant de la machine virtuelle cible de l'attaque DoS, de préserver suffisamment de ressources sur les autres machines virtuelles pour leur permettre de continuer à fonctionner.

Par défaut, ESXi impose une réservation de ressources via l'application d'un algorithme de distribution qui répartit les ressources hôte disponibles de façon équitable entre les différentes machines virtuelles, tout en conservant un certain pourcentage de ressources en vue de leur utilisation par les autres composants système. Ce comportement par défaut offre une protection naturelle efficace contre les attaques de type DoS et DDoS (Distributed Denial of Service). Vous pouvez définir les réservations et limites de ressources individuellement, ce qui permet de personnaliser le comportement par défaut pour obtenir une distribution différenciée au sein de la configuration de machines virtuelles.

Sécurité et couche réseau virtuelle

La couche de réseau virtuelle inclut des adaptateurs réseau virtuelles et des commutateurs virtuels. ESXi utilise la couche réseau virtuelle pour les communications entre les machines virtuelles et leurs utilisateurs. Par ailleurs, les hôtes utilisent cette couche pour communiquer avec les SAN iSCSI, les espaces de stockage NAS, entre autres.

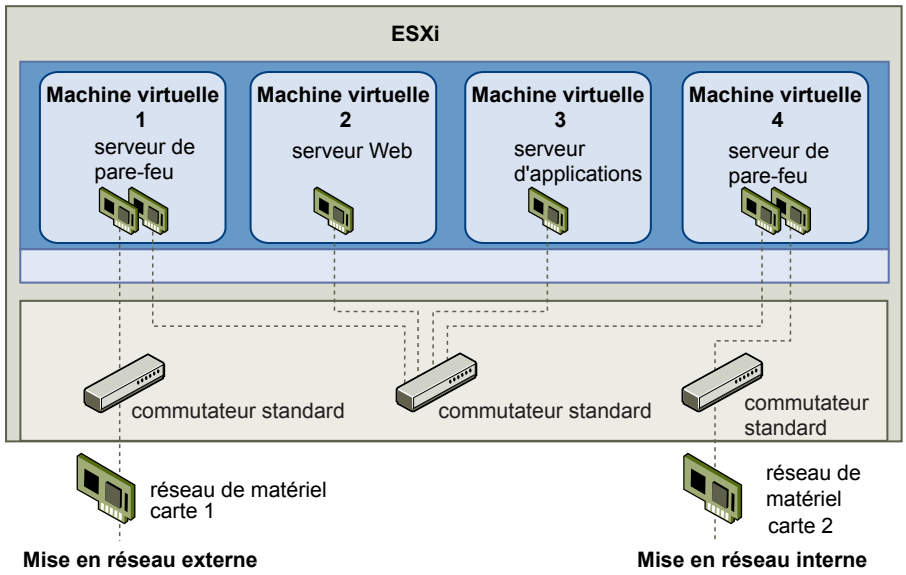
Les méthodes utilisées pour sécuriser un réseau de machines virtuelles dépendent du système d'exploitation invité installé, de la présence ou non d'un environnement sécurisé, ainsi que d'un certain nombre d'autres facteurs. Les commutateurs virtuels offrent un niveau de protection élevé lorsqu'ils sont utilisés avec d'autres mesures de sécurité (installation de pare-feu, notamment).

ESXi prend également en charge les réseaux VLAN IEEE 802.1q, que vous pouvez utiliser pour renforcer la protection du réseau de machines virtuelles ou la configuration de stockage. Les VLAN permettent de segmenter un réseau physique : ainsi, deux machines du même réseau physique peuvent s'envoyer mutuellement des paquets ou en recevoir (sauf s'ils se trouvent sur le même réseau VLAN).

Créer une DMZ réseau sur un hôte ESXi

La création d'une zone démilitarisée (DMZ) réseau sur un hôte est un exemple d'utilisation des fonctions d'isolation et de mise en réseau virtuel d'ESXi pour configurer un environnement sécurisé.

Figure 1-4. DMZ configurée sur un hôte ESXi



Dans cet exemple, quatre machines virtuelles sont configurées en vue de créer une zone démilitarisée virtuelle sur le commutateur standard 2 :

- les machines virtuelles 1 et 4 sont équipées d'un pare-feu et sont connectées à des adaptateurs virtuels via des commutateurs standard. Ces deux machines virtuelles font l'objet d'un multihébergement.
- La machine virtuelle 2 est exécutée en tant que serveur Web, tandis que la machine virtuelle 3 est exécutée en tant que serveur d'applications. Ces deux machines virtuelles font l'objet d'un hébergement mono.

Le serveur Web et le serveur d'applications occupent la DMZ entre les deux pare-feu. Le passage entre ces deux éléments est le commutateur standard 2, qui connecte les pare-feu aux serveurs. Ce commutateur ne possède pas de connexion directe aux éléments situés hors de la zone démilitarisée ; il est isolé du trafic externe via les deux pare-feu.

D'un point de vue opérationnel, le trafic externe Internet entre dans la machine virtuelle 1 via l'adaptateur réseau 1 (acheminé par le commutateur standard 1) ; il est alors vérifié par le pare-feu installé sur cette machine. Si le pare-feu autorise le trafic, celui-ci est acheminé vers le commutateur standard situé au sein de la zone démilitarisée (commutateur standard 2). Puisque le serveur Web et le serveur d'applications sont également connectés à ce commutateur, ils peuvent traiter des requêtes externes.

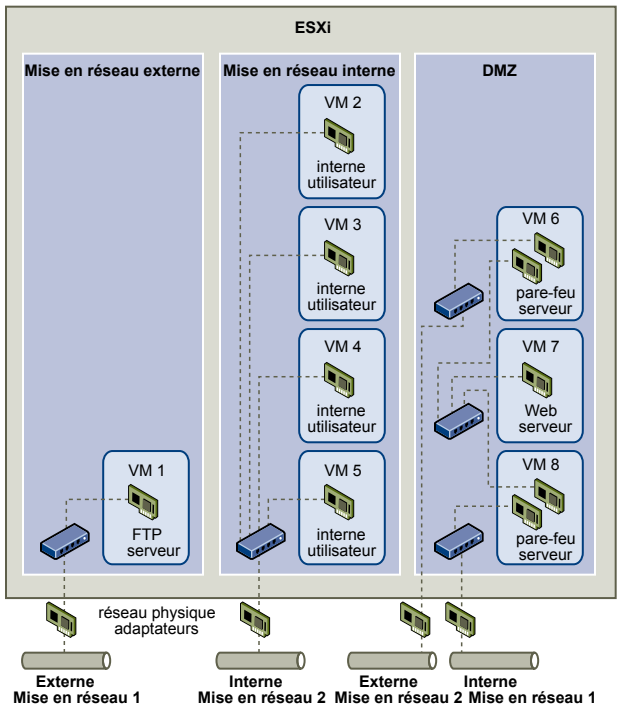
Le commutateur standard 2 est également connecté à la machine virtuelle 4. Cette machine virtuelle permet de bénéficier d'un pare-feu entre la DMZ et le réseau interne de l'entreprise. Ce pare-feu filtre les paquets en provenance du serveur Web et du serveur d'applications. Si un paquet est vérifié, il est acheminé vers l'adaptateur réseau 2 via le commutateur standard 3. L'adaptateur réseau 2 est connecté au réseau interne de l'entreprise.

Lorsque vous créez une DMZ sur un seul hôte, vous pouvez utiliser des pare-feu assez légers. Dans cette configuration, une machine virtuelle ne peut pas exercer un contrôle direct sur une autre machine virtuelle, ni accéder à sa mémoire ; toutefois, toutes les machines virtuelles restent connectées via un réseau virtuel. Or, ce réseau peut être utilisé pour la propagation de virus ou être la cible d'autres types d'attaques. La sécurité des machines virtuelles dans la zone démilitarisée revient donc à séparer les machines physiques connectées au même réseau.

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 1-5. 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 via l'examen de la disposition des commutateurs réseau dans vSphere 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.

Ressources de sécurité et informations

Pour obtenir des informations complémentaires sur la sécurité, consultez le site Web de VMware.

Le tableau répertorie les rubriques liées à la sécurité et indique l'emplacement des informations complémentaires correspondantes.

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

Rubrique	Ressource
Politique de sécurité VMware, alertes de sécurité actualisées, téléchargements de sécurité et discussions sur des thèmes liés à la sécurité	http://www.vmware.com/fr/technical-resources/virtualization-topics/security
Politique de l'entreprise en matière de réponse sécuritaire	http://www.vmware.com/fr/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.
Politique de support logiciel tiers	http://www.vmware.com/fr/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 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.

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

Rubrique	Ressource
Information générale sur la virtualisation et la sécurité	Centre virtuel de ressources techniques de sécurité VMware http://www.vmware.com/fr/technical-resources/virtualization-topics/security
Standards de sécurité et de conformité, ainsi que solutions partenaires et contenu détaillé sur la virtualisation et la conformité	http://www.vmware.com/fr/technical-resources/virtualization-topics/security/compliance
Informations sur la technologie de protection de machines virtuelles VMsafe, incluant une liste de solutions partenaires	http://www.vmware.com/fr/technical-resources/virtualization-topics/security/vmsafe/security_technology

Sécurisation des configurations d' ESXi 2

Vous pouvez prendre des mesures pour promouvoir un environnement sécurisé pour vos hôtes ESXi, vos machines virtuelles et vos SAN iSCSI. Prenez en compte la planification de la configuration réseau du point de vue de la sécurité et les mesures que vous pouvez prendre pour protéger les composants de votre configuration des attaques.

Ce chapitre aborde les rubriques suivantes :

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 toutes les voies de communication, excepté pour celles que l'administrateur désigne explicitement ou implicitement comme autorisées. Les voies, ou ports, que les administrateurs ouvrent dans le pare-feu autorisent le trafic entre les périphériques sur les différents côtés du pare-feu.

Important Le pare-feu ESXi d'ESXi 5.0 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.

- Les machines physiques telles que les systèmes vCenter Server et les hôtes ESXi.
- Une machine virtuelle et une autre (par exemple, entre une machine virtuelle agissant en tant que serveur Web externe et une machine virtuelle connectée à votre réseau interne de l'entreprise).
- Une machine physique et une machine virtuelle, notamment lorsque vous placez un pare-feu entre un adaptateur réseau physique et une machine virtuelle.

La manière dont vous utilisez 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 sur un hôte externe, vous devez définir la configuration afin qu'un pare-feu soit présent au point d'entrée du réseau virtuel pour protéger tout l'ensemble de machines virtuelles.

Pare-feux pour configurations avec vCenter Server

Si vous accédez aux hôtes ESXi via vCenter Server, vous protégez généralement vCenter Server avec un pare-feu. Ce pare-feu fournit une protection de base à votre réseau.

Un pare-feu peut se trouver entre les clients et vCenter Server. vCenter Server et les clients peuvent se trouver également derrière un pare-feu, en fonction de votre déploiement. L'important est de s'assurer qu'un pare-feu est présent sur ce que vous considérez être un point d'entrée pour le système.

Pour obtenir la liste complète des ports TCP et UDP, y compris ceux de vSphere vMotion™ et vSphere Fault Tolerance, consultez « Ports TCP et UDP pour l'accès de gestion », page 21.

Les réseaux configurés avec vCenter Server peuvent recevoir des communications via vSphere Client ou des clients de gestion réseau tiers utilisant SDK pour communiquer avec l'hôte. En fonctionnement normal, vCenter Server écoute les données de ses hôtes gérés et de ses clients sur les ports indiqués. vCenter Server suppose également que ses hôtes gérés écoutent les données de vCenter Server sur les ports indiqués. 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 à un grand nombre d'autres points d'accès du réseau, en fonction de la manière dont vous envisagez d'utiliser le réseau et du niveau de sécurité nécessaire aux différents périphériques. Sélectionnez les emplacements de vos pare-feu en fonction des risques de sécurité que vous avez identifiés pour votre configuration réseau. Vous trouverez ci-après une liste des emplacements de pare-feu commune aux implémentations ESXi.

- Entre vSphere Client ou un client de gestion 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 aux machines virtuelles via vSphere Client, entre vSphere Client et l'hôte ESXi. Cette connexion s'ajoute à la connexion entre vSphere 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 envisagez de migrer les machines virtuelles entre les serveurs, faites un clonage ou utilisez vMotion. Vous devez également ouvrir des ports dans les pare-feu qui divisent l'hôte source des hôtes cibles afin que la source et les cibles puissent communiquer.
- 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.

Pare-feu pour configurations sans vCenter Server

Si vous connectez des clients directement à votre réseau ESXi au lieu d'utiliser vCenter Server, la configuration de votre pare-feu est assez simple.

Les réseaux configurés sans vCenter Server reçoivent des communications par l'intermédiaire des mêmes types de clients que si vCenter Server était présent : vSphere Client ou des clients de gestion de réseau tiers. Les besoins du pare-feu sont en majeure partie identiques, mais il y a plusieurs différences clés.

- Tout comme pour les configurations comprenant vCenter Server, assurez-vous qu'un pare-feu est présent pour protéger votre couche ESXi ou, en fonction de votre configuration, vos clients et votre couche ESXi. Ce pare-feu fournit une protection de base à votre réseau. Les ports du pare-feu que vous utilisez sont identiques à ceux que vous utiliseriez si vCenter Server était présent.
- La licence pour ce type de configuration fait partie du module ESXi que vous installez sur chacun des hôtes. Comme la licence réside sur le serveur, un serveur de licences distinct n'est pas nécessaire. Un pare-feu entre le serveur de licences et le réseau ESXi n'est donc pas nécessaire.

Connexion à vCenter Server via un pare-feu

Le port que vCenter Server utilise pour écouter le transfert de données de son client est le port 443. Si un pare-feu se trouve entre vCenter Server et ses clients, vous devez configurer une connexion au travers de laquelle vCenter Server peut recevoir des données à partir des clients.

Pour permettre à vCenter Server de recevoir des données de vSphere Client, ouvrez le port 443 dans le pare-feu pour permettre le transfert de données de vSphere Client vers vCenter Server. Contactez l'administrateur système du pare-feu pour plus d'informations sur la configuration des ports dans un pare-feu.

Si vous utilisez vSphere Client et que vous ne souhaitiez pas utiliser le port 443 comme port pour la communication client à vCenter Server, vous pouvez passer sur un autre port en modifiant les paramètres vCenter Server dans vSphere Client. Pour en savoir plus sur la manière de modifier ces paramètres, consultez la documentation *Gestion de vCenter Server et des hôtes*.

Connexion à la console de la machine virtuelle via un pare-feu

Lorsque vous connectez votre client à des hôtes ESXi via vCenter Server ou utilisez une connexion directe à l'hôte, certains ports sont requis pour la communication utilisateur et administrateur avec les consoles des machines virtuelles. Ces ports prennent en charge différentes fonctions client, communiquent avec différentes couches sur ESXi et utilisent différents protocoles d'authentification.

Port 902

Il s'agit du port que vCenter Server considère comme disponible pour la réception des données provenant d'ESXi. vSphere Client utilise ce port pour fournir une connexion pour les activités de la souris, du clavier, de l'écran (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. Le port 902 est le port que vSphere Client considère comme disponible pour l'interaction avec les machines virtuelles.

Le port 902 connecte vCenter Server à l'hôte via VMware Authorization Daemon (`vmware-authd`). Ce démon multiplexe les données du port 902 au destinataire approprié pour le traitement. VMware ne prend pas en charge la configuration d'un port différent pour cette connexion.

Port 443

vSphere Client et SDK utilisent ce port pour envoyer des données aux hôtes gérés par vCenter Server. Par conséquent, vSphere Client et SDK, s'ils sont connectés directement à ESXi, utilisent ce port pour prendre en charge toutes les fonctions de gestion relatives au serveur et à ses machines virtuelles. Le port 443 est le port que les clients considèrent comme disponible lors de l'envoi de données à ESXi. VMware ne prend pas en charge la configuration d'un port différent pour ces connexions.

Le port 443 connecte les clients à l'hôte ESXi via le service Web Tomcat ou SDK. Le processus hôte multiplexe les données du port 443 au destinataire approprié pour le traitement.

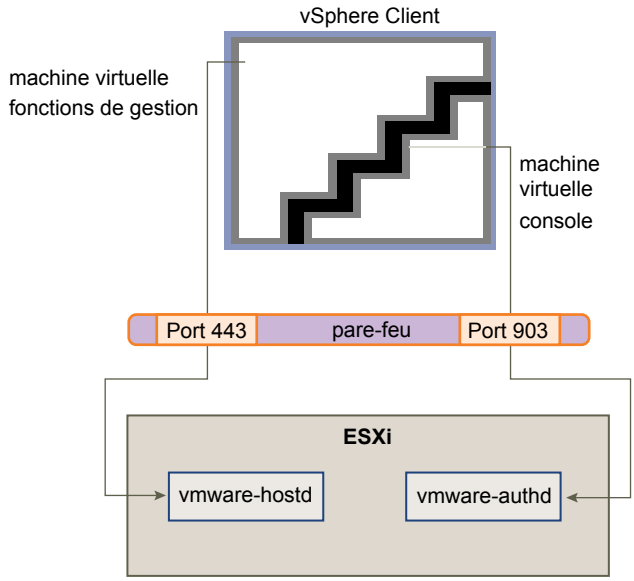
Port 903

vSphere Client utilise ce port pour fournir une connexion pour les 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. Le port 903 est le port que vSphere Client considère comme disponible pour l'interaction avec les machines virtuelles. VMware ne prend pas en charge la configuration d'un port différent pour cette fonction.

Le port 903 connecte vSphere Client à une machine virtuelle spécifique configurée sur ESXi.

L'image qui suit présente les relations entre les fonctions de vSphere Client, les ports et les processus.

Figure 2-1. Utilisation des ports pour les communications client avec ESXi



Si un pare-feu se trouve entre votre système vCenter Server et l'hôte géré par vCenter Server, ouvrez les ports 443 et 903 du pare-feu pour permettre le transfert des données aux hôtes ESXi à partir de vCenter Server et aux hôtes ESXi à partir de vSphere Client.

Pour plus d'informations sur la configuration des ports, consultez l'administrateur système du pare-feu.

Connexion des hôtes ESXi via des pare-feu

Si un pare-feu se trouve entre deux hôtes ESXi et que vous souhaitez autoriser des transactions entre les hôtes ou utiliser vCenter Server pour effectuer des activités sources ou cibles, telles que du trafic vSphere High Availability (vSphere HA), une migration, un clonage ou vMotion, vous devez configurer une connexion par laquelle 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 « Ports TCP et UDP pour l'accès de gestion », page 21 pour obtenir une liste de ports. Consultez l'administrateur système du pare-feu pour plus d'informations sur la configuration des ports.

Ports TCP et UDP pour l'accès de gestion

vCenter Server, les hôtes ESXi et d'autres composants réseau sont accessibles à l'aide 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.

Le tableau répertorie les ports TCP et UDP et l'objectif et le type de chaque port. Les ports qui sont ouverts par défaut lors de l'installation sont suivis de la mention « (par défaut) ».

Tableau 2-1. Ports TCP et UDP

Port	Objectif	Type de trafic
22 (par défaut)	Serveur SSH	TCP entrant
53 (par défaut)	Client DNS	UDP entrant et sortant
68 (par défaut)	Client DHCP	UDP entrant et sortant
161 (par défaut)	serveur SNMP	UDP entrant
80 (par défaut)	vSphere Fault Tolerance (FT) (TCP sortant, UDP) Accès HTTP Port Web TCP non sécurisé par défaut généralement utilisé en association avec le port 443 comme serveur frontal pour accéder aux réseaux ESXi à partir du Web. Le port 80 redirige le trafic vers une page de destination HTTPS (port 443). Gestion WS	TCP entrant TCP sortant, UDP
123	Client NTP	UDP sortant
427 (par défaut)	Le client CIM utilise le Service Location Protocol, version 2 (SLPv2) pour rechercher des serveurs CIM.	UDP entrant et sortant
443 (par défaut)	Accès HTTPS Accès vCenter Server aux hôtes ESXi Port Web SSL par défaut Accès vSphere Client à vCenter Server Accès vSphere Client aux hôtes ESXi Gestion WS Accès vSphere Client à vSphere Update Manager Connexions clients de gestion de réseau tiers à vCenter Server Accès clients de gestion de réseau tiers à des hôtes	TCP entrant
902 (par défaut)	Accès de l'hôte aux autres hôtes pour la migration et l'approvisionnement Trafic d'authentification pour ESXi et trafic de la console distante (xinetd/vmware-authd) Accès vSphere Client aux consoles des machines virtuelles Connexion (pulsation) de mise à niveau d'état (UDP) à partir dESXi vers vCenter Server	TCP entrant et sortant, UDP sortant

Tableau 2-1. Ports TCP et UDP (suite)

Port	Objectif	Type de trafic
903	Trafic de la console distante généré par l'accès utilisateur aux machines virtuelles sur un hôte spécifique. Accès vSphere Client aux consoles des machines virtuelles Transactions MKS (xinetd/vmware-authd-mks)	TCP entrant
1234, 1235 (par défaut)	HBR	TCP sortant
2049	Transactions provenant des périphériques de stockage NFS Ce port est utilisé sur l'interface VMkernel.	UDP entrant et sortant
2050–2250	Trafic entre les hôtes pour vSphere High Availability (vSphere HA) et EMC Autostart Manager	TCP sortant, UDP entrant et sortant
3260	Transactions vers les périphériques de stockage iSCSI	TCP sortant
5900-5964	Protocole RFB qui est utilisé par les outils de gestion tels que VNC	UDP entrant et sortant
5988 (par défaut)	Transactions CIM sur HTTP	TCP entrant
5989 (par défaut)	Transactions XML CIM sur HTTPS	UDP entrant et sortant
8000 (par défaut)	Requêtes de vMotion	UDP entrant et sortant
8042–8045	Trafic entre les hôtes pour HA et EMC Autostart Manager	TCP sortant, UDP entrant et sortant
8100, 8200 (par défaut)	Trafic entre les hôtes pour vSphere Fault Tolerance (FT)	TCP entrant et sortant, UDP

En plus des ports TCP et UDP, vous pouvez configurer d'autres ports en fonction de vos besoins.

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. Vous pouvez augmenter la sécurité de votre réseau de machines virtuelles de différentes manières.

Si votre réseau de machines virtuelles est connecté à un réseau physique, il peut être soumis à des défaillances du même degré qu'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.

Vous pouvez ajouter ce niveau de sécurité de différentes manières.

- Ajout d'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. Cela sert de tampon de protection entre l'adaptateur réseau physique et les machines virtuelles restantes du réseau virtuel.

L'installation d'un pare-feu hébergé sur hôte sur les machines virtuelles à la tête des réseaux virtuels est une bonne pratique de sécurité. Cependant, comme les pare-feu hébergés sur hôte peuvent ralentir les performances, équilibrez vos besoins en sécurité par rapport aux performances avant de décider d'installer des pare-feu hébergés sur hôte sur des machines virtuelles ailleurs dans le réseau virtuel.

- Conservation de différentes zones de machines virtuelles au sein d'un hôte sur différents segments du réseau. Si vous isolez des zones de machines virtuelles sur leurs propres segments de réseau, vous réduisez les risques 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 attaquants utilisent l'usurpation ARP pour générer des dénis de service, pirater le système cible et interrompre le réseau virtuel.

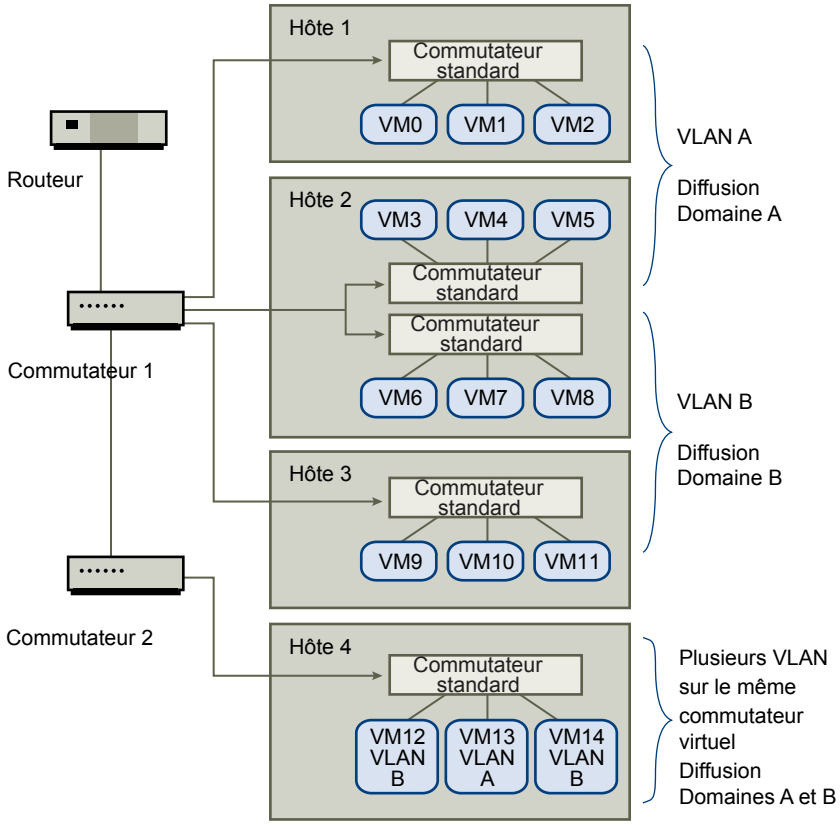
  La planification soignée de la segmentation réduit les chances de transmissions de paquets entre les zones de machines virtuelles, ce qui empêche les attaques de reniflement qui nécessitent l'envoi de trafic réseau à la victime. Par conséquent, un attaquant ne peut pas utiliser un service non sécurisé 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.

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 2-2. 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.

VLAN faisant partie d'une plus vaste implémentation de sécurité

Les VLAN sont des moyens efficaces de contrôler où et dans quelle mesure les données sont transmises sur le réseau. Si un attaquant parvient à accéder au réseau, il est susceptible d'être restreint au VLAN servant de point d'entrée, réduisant le risque encouru par le réseau dans sa globalité.

Les VLAN fournissent une protection uniquement par le fait qu'ils contrôlent la manière dont les données sont acheminées après avoir traversé les commutateurs et être entrées dans le réseau. Vous pouvez utiliser des VLAN pour sécuriser la couche 2 de votre architecture réseau (couche de liaison de données). Cependant, la configuration des VLAN ne protège pas la couche physique de votre modèle réseau ou tout autre couche. Même si vous créez des VLAN, fournissez une protection supplémentaire en sécurisant votre matériel (routeurs, hub, etc.) et en chiffrant les transmissions de données.

Les VLAN ne remplacent pas les pare-feu dans vos configurations de machines virtuelles. La plupart des configurations réseau comprenant des VLAN incluent également des pare-feu. Si vous incluez des VLAN dans votre réseau virtuel, assurez-vous que les pare-feu que vous installez prennent en charge les VLAN.

Configuration correcte des VLAN

Une configuration incorrecte de l'équipement et des défauts du matériel réseau, des microprogrammes ou des logiciels risquent de créer un VLAN susceptible de subir des attaques VLAN Hopping.

Le VLAN hopping survient lorsqu'un attaquant avec accès autorisé à un VLAN crée des paquets qui simulent des commutateurs physiques en transmettant des paquets à un autre VLAN auquel l'attaquant n'est pas autorisé à accéder. La vulnérabilité à ce type d'attaque provient généralement d'un commutateur mal configuré pour un fonctionnement en VLAN natif, dans lequel le commutateur peut recevoir et transmettre des paquets non marqués.

Pour empêcher le VLAN hopping, conservez votre équipement à niveau en installant les mises à jour matérielles et des microprogrammes au fur et à mesure de leur mise à disposition. Par conséquent, respectez les recommandations des meilleures pratiques de votre fournisseur lorsque vous configurez votre équipement.

Les commutateurs standard VMware ne prennent pas en charge le concept de VLAN natif. Toutes les données transmises à ces commutateurs sont marquées de manière adéquate. Cependant, comme les autres commutateurs du réseau peuvent être configurés pour un fonctionnement en VLAN natif, les VLAN configurés avec des commutateurs standard peuvent toujours être vulnérables au VLAN hopping.

Si vous envisagez d'utiliser des VLAN pour renforcer la sécurité du réseau, désactivez la fonction de VLAN natif pour tous les commutateurs à moins que vous n'ayez une raison impérative pour faire fonctionner les VLAN en mode natif. Si vous devez utiliser un VLAN natif, reportez-vous aux consignes de configuration du fournisseur pour cette fonction.

Protection des commutateurs standard et VLAN

Les commutateurs standard VMware assurent une protection contre certaines menaces pour la sécurité du VLAN. En raison de la manière dont certains commutateurs standard sont conçus, ils protègent les VLAN contre un grand nombre d'attaques, dont un grand nombre implique le VLAN hopping.

Disposer de cette protection ne garantit pas que la configuration de vos machines virtuelles n'est pas vulnérable à d'autres types d'attaques. Par exemple, les commutateurs standard ne protègent pas le réseau physique contre ces attaques : ils protègent uniquement le réseau virtuel.

Les commutateurs standard et les VLAN peuvent protéger des types d'attaques suivants.

Saturation MAC

Saturation d'un commutateur avec des paquets contenant des adresses MAC balisées comme provenant de sources différentes. De nombreux commutateurs utilisent une table de mémoire adressable par contenu pour détecter et stocker l'adresse source de chaque paquet. Lorsque la table est pleine, le commutateur peut passer dans un état totalement ouvert dans lequel chaque paquet entrant est diffusé sur tous les ports, permettant à l'attaquant de voir tout le trafic du commutateur. Cet état peut provoquer une fuite des paquets sur les VLAN.

Bien que les commutateurs standard de VMware stockent la table d'adresses MAC, ils n'obtiennent pas les adresses MAC du trafic observable et ne sont pas vulnérables à ce type d'attaque.

Attaques 802.1q et de balisage ISL

Force un commutateur à rediriger des cadres d'un VLAN à un autre en amenant le commutateur à agir comme un tronçon et à diffuser le trafic aux autres VLAN.

Les commutateurs standard de VMware n'effectuent pas la jonction dynamique requise pour ce type d'attaque et ne sont pas par conséquent vulnérables.

Attaques à double encapsulation

Survient lorsqu'un attaquant crée un paquet à double encapsulation dans lequel l'identifiant de VLAN dans la balise interne est différent de l'identifiant de VLAN dans la balise externe. Pour des raisons de compatibilité descendante, les VLAN natifs ôtent la balise externe des paquets transmis sauf s'ils sont configurés pour ne pas le faire. Lorsque le commutateur d'un VLAN natif ôte la balise externe, seule la balise interne reste et cette balise interne achemine le paquet à un VLAN différent de celui identifié par la balise externe maintenant manquante.

Les commutateurs standard de VMware rejettent les cadres à double encapsulation qu'une machine virtuelle tente d'envoyer sur un port configuré pour un VLAN spécifique. Par conséquent, ils ne sont pas vulnérables à ce type d'attaque.

Attaques de force brute multidiffusion

Implique l'envoi d'un grand nombre de cadres multidiffusion à un VLAN connu presque simultanément pour surcharger le commutateur afin qu'il autorise par erreur la diffusion de certains cadres sur d'autres VLAN.

Les commutateurs standard de VMware ne permettent pas aux cadres de quitter leur domaine de diffusion correspondant (VLAN) et ne sont pas vulnérables à ce type d'attaque.

Attaques l'arbre recouvrant

Spanning-Tree Protocol (STP) cible, qui est utilisé pour contrôler le pontage entre des parties du LAN. L'attaquant envoie des paquets Bridge Protocol Data Unit (BPDU) qui tentent de modifier la topologie du réseau, en se définissant comme le pont racine. En tant que pont racine, l'attaquant peut renifler le contenu des cadres transmis.

Les commutateurs standard de VMware ne prennent pas en charge STP et ne sont pas vulnérables à ce type d'attaque.

Attaques à trame aléatoire

Implique l'envoi d'un grand nombre de paquets dans lesquels les adresses de source et de destination restent identiques, mais dans lesquels les zones sont modifiées aléatoirement en longueur, type ou contenu. L'objectif de cette attaque est de forcer les paquets à être réacheminés par erreur vers un VLAN différent.

Les commutateurs standard de VMware ne sont pas vulnérables à ce type d'attaque.

Comme de nouvelles menaces de sécurité continuent à se développer, ne considérez pas cela comme une liste exhaustive des attaques. Vérifiez régulièrement les ressources de sécurité de VMware sur le Web pour en savoir plus sur la sécurité, les alertes de sécurité récentes et les tactiques de sécurité de VMware.

Sécurisation des ports de commutateurs standard

Tout comme pour les adaptateurs réseau physiques, un adaptateur réseau virtuel peut envoyer des cadres qui semblent provenir d'une machine différente ou emprunter l'identité d'une autre machine afin de pouvoir recevoir des cadres réseau destinés à cette machine. Par conséquent, tout comme les adaptateurs réseau physiques, un adaptateur réseau virtuel peut être configuré afin de recevoir des cadres destinés à d'autres machines.

Lorsque vous créez un commutateur standard pour votre réseau, vous ajoutez des groupes de ports pour imposer une configuration de règles pour les machines virtuelles et les systèmes de stockage reliés au commutateur. Vous créez des ports virtuels via vSphere Client.

Dans le cadre de l'ajout d'un port ou d'un groupe de ports à un commutateur standard, vSphere Client configure un profil de sécurité pour le port. 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.

Le profil de sécurité détermine le niveau de puissance 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 les bases du contrôle des transmissions par les adaptateurs réseau virtuels et la manière dont les attaques sont bloquées à ce niveau.

Chaque adaptateur réseau virtuel a sa propre adresse MAC qui lui est attribuée lors de la création de l'adaptateur. Cette adresse est appelée adresse MAC initiale. 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. Par ailleurs, 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 l'envoi de paquets, un système d'exploitation place généralement l'adresse MAC effective de son propre adaptateur réseau dans la zone de l'adresse MAC source du cadre Ethernet. Il place également l'adresse MAC pour l'adaptateur réseau récepteur dans la zone d'adresse MAC de destination. L'adaptateur récepteur accepte les paquets uniquement lorsque l'adresse MAC de destination dans le paquet correspond à sa propre adresse MAC effective.

Lors de la création, l'adresse MAC effective de l'adaptateur réseau et l'adresse MAC initiale sont identiques. Le système d'exploitation de la machine virtuelle peut remplacer l'adresse MAC effective par une autre valeur à tout moment. Si un système d'exploitation modifie l'adresse MAC effective, son adaptateur réseau reçoit le trafic réseau destiné à la nouvelle adresse MAC. Le système d'exploitation peut envoyer des cadres avec une adresse MAC source usurpée à tout moment. 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.

Vous pouvez utiliser des profils de sécurité de commutateur standard sur les hôtes pour vous protéger contre ce type d'attaque en définissant trois options. Si vous modifiez un paramètre par défaut pour un port, vous devez modifier le profil de sécurité en éditant les paramètres du commutateur standard dans vSphere Client.

Modifications d'adresse MAC

Le paramètre pour l'option **[Modifications d'adresse MAC]** affecte le trafic qu'une machine virtuelle reçoit.

Lorsque cette option 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 cette option 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, qui protège l'hôte contre l'emprunt d'identité MAC. Le port que l'adaptateur virtuel a utilisé pour envoyer la demande est désactivé et l'adaptateur virtuel ne reçoit plus de cadres jusqu'à ce que l'adresse MAC effective soit remplacée par l'adresse MAC initiale. Le système d'exploitation invité ne détecte pas que le changement d'adresse MAC n'a pas été honoré.

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 et avez 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.

Les paramètres de changement des adresses MAC affectent le trafic sortant d'une machine virtuelle. Les modifications d'adresse MAC surviennent si l'émetteur est autorisé à les faire, même si les commutateurs standard ou une machine virtuelle réceptrice ne permet pas les changements d'adresses MAC.

Transmissions forgées

Le paramètre pour l'option **[Transmissions forcées :]** affecte le trafic transmis à partir d'une machine virtuelle.

Lorsque cette option est définie sur **[Accepter]**, ESXi ne compare pas les adresses MAC sources et les adresses MAC effectives.

Pour se protéger d'un emprunt d'identité MAC, vous pouvez définir cette option sur **[Rejeter]**. Si vous effectuez cette opération, l'hôte compare l'adresse MAC source étant transmise par le système d'exploitation avec l'adresse MAC effective pour son adaptateur pour voir si elles correspondent. Si les adresses ne correspondent pas, ESXi rejette le paquet.

Le système d'exploitation invité ne détecte pas que son adaptateur de réseau virtuel 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 le filtrage de réception que l'adaptateur de réseau virtuel effectuerait afin que le système d'exploitation invité reçoive tout le trafic observé sur le réseau. Par défaut, l'adaptateur de réseau virtuel 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 standard pour fonctionner en mode promiscuité (par exemple, si vous exécutez un logiciel de détection des intrusions réseau ou un renifleur de paquets).

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 avec 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 de chiffrer le trafic IP dépend de la manière dont vous configurez les associations de sécurité du système et les stratégies de sécurité.

Une association de sécurité détermine comment le système chiffre le trafic. Lorsque vous créez une association de sécurité, vous spécifiez la source et la destination, les paramètres de chiffrement, un nom pour 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.

Ajout d'une association de sécurité

Ajoutez une association de sécurité pour définir des paramètres de chiffrement pour le trafic IP associé.

Vous pouvez ajouter une association de sécurité à l'aide de la commande `vicfg-ipsec` de vSphere CLI.

Dans la procédure, **`--server=`*`server_name`*** spécifie le serveur cible. Le serveur cible spécifié vous invite à saisir un nom de serveur et un mot de passe. D'autres options de connexion, telles qu'un fichier de configuration ou de session, sont prises en charge. Pour obtenir une liste des options de connexion, reportez-vous à *Initiation aux interfaces de ligne de commande vSphere*.

Prérequis

Installez vCLI ou déployez la machine virtuelle de vSphere Management Assistant (vMA). Reportez-vous à la section *Initiation aux interfaces de ligne de commande vSphere*. Pour le dépannage, exécutez les commandes `esxcli` dans ESXi Shell.

Procédure

- Dans l'invite de commande, saisissez **`vicfg-ipsec --server=`*`server_name`*` --add-sa`** avec une ou plusieurs des options suivantes.

Option	Description
`--sa-src` ***source address***	Spécifiez l'adresse source.
`--sa-dst` ***destination address***	Spécifiez l'adresse de destination.

Option	Description
`--sa-mode` ***mode***	Spécifiez le mode, soit `transport` ou `tunnel`.
`--spi` ***security parameter index***	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.
`--ealgo` ***encryption algorithm***	Spécifiez l'algorithme de chiffrement à l'aide d'un des paramètres suivants. ■ `3des-cbc` ■ `aes128-cbc` ■ `null` `null` aucun chiffrement.
`--ekey` ***encryption key***	Spécifiez la clé de chiffrement. Vous pouvez entrer des clés en tant que texte ASCII ou en tant qu'hexadécimal avec un préfixe 0x.
`--ialgo` ***authentication algorithm***	Spécifiez l'algorithme d'authentification, soit `hmac-sha1` ou `hmac-sha2-256`.
`--ikey` ***authentication key***	Spécifiez la clé d'authentification. Vous pouvez entrer des clés en tant que texte ASCII ou en tant qu'hexadécimal avec un préfixe 0x.
name	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.

```
vicfg-ipsec --server=server_name --add-sa
--sa-src 3ffe:501:ffff:0::a
--sa-dst 3ffe:501:ffff:0001:0000:0000:0000:0001
--sa-mode transport
--spi 0x1000
--ealgo 3des-cbc
--ekey 0x697076367265616479 6c6f676f336465736362636f757432
--ialgo hmac-sha1
--ikey 0x697076367265616479 6c6f67736861316f757432
sa1
```

Suppression d'une association de sécurité

Vous pouvez supprimer une association de sécurité de l'hôte.

Vous pouvez supprimer une association de sécurité à l'aide de la commande `vicfg-ipsec`.

Dans la procédure, `--server=`***`server_name`*** spécifie le serveur cible. Le serveur cible spécifié vous invite à saisir un nom de serveur et un mot de passe. D'autres options de connexion, telles qu'un fichier de configuration ou de session, sont prises en charge. Pour obtenir une liste des options de connexion, reportez-vous à *Initiation aux interfaces de ligne de commande vSphere*.

Prérequis

Assurez-vous que l'association de sécurité que vous souhaitez utiliser n'est pas actuellement utilisée. Si vous essayez de supprimer une association de sécurité en cours d'utilisation, l'opération de suppression échoue.

Installez vCLI ou déployez la machine virtuelle de vSphere Management Assistant (vMA). Reportez-vous à la section *Initiation aux interfaces de ligne de commande vSphere*. Pour le dépannage, exécutez les commandes `esxcli` dans ESXi Shell.

Procédure

- Dans l'invite de commande, saisissez **`vicfg-ipsec --server=`*`server_name`*** **`--remove-sa`** ***`security_association_name`***.

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 `vicfg-ipsec`.

Dans la procédure, **`--server=`*`server_name`*** spécifie le serveur cible. Le serveur cible spécifié vous invite à saisir un nom de serveur et un mot de passe. D'autres options de connexion, telles qu'un fichier de configuration ou de session, sont prises en charge. Pour obtenir une liste des options de connexion, reportez-vous à *Initiation aux interfaces de ligne de commande vSphere*.

Prérequis

Installez vCLI ou déployez la machine virtuelle de vSphere Management Assistant (vMA). Reportez-vous à la section *Initiation aux interfaces de ligne de commande vSphere*. Pour le dépannage, exécutez les commandes `esxcli` dans ESXi Shell.

Procédure

- Dans l'invite de commande, saisissez **`vicfg-ipsec --server=`*`server_name`*** **`-l`**.

ESXi affiche une liste de toutes les associations de sécurité disponibles.

Création d'une règle de sécurité

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 règle de sécurité à l'aide de la commande `vicfg-ipsec` de vSphere CLI.

Dans la procédure, **`--server=`*`server_name`*** spécifie le serveur cible. Le serveur cible spécifié vous invite à saisir un nom de serveur et un mot de passe. D'autres options de connexion, telles qu'un fichier de configuration ou de session, sont prises en charge. Pour obtenir une liste des options de connexion, reportez-vous à *Initiation aux interfaces de ligne de commande vSphere*.

Prérequis

Avant de créer une règle de sécurité, ajoutez une association de sécurité comportant les paramètres d'authentification et de chiffrement appropriés décrits dans « Ajout d'une association de sécurité », page 29.

Installez vCLI ou déployez la machine virtuelle de vSphere Management Assistant (vMA). Reportez-vous à la section *Initiation aux interfaces de ligne de commande vSphere*. Pour le dépannage, exécutez les commandes `esxcli` dans ESXi Shell.

Procédure

- Dans l'invite de commande, saisissez **`vicfg-ipsec --server=`*`server_name`*** **`--add-sp`** et une ou plusieurs des options suivantes.

Option	Description
`--sp-src` ***source address***	Spécifiez l'adresse IP source et la longueur du préfixe.
`--sp-dst` ***destination address***	Spécifiez l'adresse de destination et la longueur du préfixe.
`--src-port` ***port***	Spécifiez le port source. Le port source doit être un nombre compris entre 0 et 65 535.

Option	Description
--dst-port ***port***	Spécifiez le port de destination. Le port source doit être un nombre compris entre 0 et 65 535.
--ulproto ***protocol***	Spécifiez le protocole de couche supérieure à l'aide d'un des paramètres suivants. ■ `tcp` ■ `udp` ■ `icmp6` ■ `toutes`
--dir ***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***	Indiquez le nom de l'association de sécurité pour la règle de sécurité à utiliser.
name	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.

```
vicfg-ipsec --server=server_name --add-sp
--sp-src 2001:db8:1::/64
--sp-dst 2002:db8:1::/64
--src-port 23
--dst-port 25
--ulproto tcp
--dir out
--action ipsec
--sp-mode transport
--sa-name sa1
sp1
```

Suppression d'une règle de sécurité

Vous pouvez supprimer une règle de sécurité de l'hôte ESXi.

Vous pouvez supprimer une règle de sécurité à l'aide de la commande `vicfg-ipsec`.

Dans la procédure, **--server=*server_name*** spécifie le serveur cible. Le serveur cible spécifié vous invite à saisir un nom de serveur et un mot de passe. D'autres options de connexion, telles qu'un fichier de configuration ou de session, sont prises en charge. Pour obtenir une liste des options de connexion, reportez-vous à *Initiation aux interfaces de ligne de commande vSphere*.

Prérequis

Assurez-vous que la règle 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.

Installez vCLI ou déployez la machine virtuelle de vSphere Management Assistant (vMA). Reportez-vous à la section *Initiation aux interfaces de ligne de commande vSphere*. Pour le dépannage, exécutez les commandes `esxcli` dans ESXi Shell.

Procédure

- Dans l'invite de commande, saisissez **`vicfg-ipsec server=`*`server_name`*` --remove-sp `*`security_policy_name`***.

Liste des règles de sécurité disponibles

ESXi peut fournir une liste de toutes les règles de sécurité de l'hôte.

Vous pouvez obtenir une liste des règles de sécurité disponibles à l'aide de la commande `vicfg-ipsec`.

Dans la procédure, **`--server=`*`server_name`*** spécifie le serveur cible. Le serveur cible spécifié vous invite à saisir un nom de serveur et un mot de passe. D'autres options de connexion, telles qu'un fichier de configuration ou de session, sont prises en charge. Pour obtenir une liste des options de connexion, reportez-vous à *Initiation aux interfaces de ligne de commande vSphere*.

Prérequis

Installez vCLI ou déployez la machine virtuelle de vSphere Management Assistant (vMA). Reportez-vous à la section *Initiation aux interfaces de ligne de commande vSphere*. Pour le dépannage, exécutez les commandes `esxcli` dans ESXi Shell.

Procédure

- Dans l'invite de commande, saisissez **`vicfg-ipsec --server=`*`server_name`*` -L`**.

L'hôte affiche une liste de toutes les règles de sécurité disponibles.

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 via l'authentification

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 le LUN cible.

L'objectif de l'authentification est de prouver que l'initiateur a le droit d'accéder à une cible, droit accordé lorsque vous configurez l'authentification.

ESXi ne prend pas en charge Kerberos, Secure Remote Protocol (SRP) ou les méthodes d'authentification par clé publique d'iSCSI. Par ailleurs, il ne prend pas en charge l'authentification IPsec et le chiffrement.

Utilisez vSphere Client pour déterminer si l'authentification est effectuée et pour configurer la méthode d'authentification.

Activation du CHAP (Challenge Handshake Authentification Protocol) pour les SAN iSCSI

Vous pouvez configurer le SAN iSCSI pour utiliser l'authentification CHAP.

Dans l'authentification CHAP, lorsque l'initiateur contacte une cible iSCSI, la cible envoie une valeur d'ID prédéfinie et une valeur aléatoire, ou clé, à l'initiateur. L'initiateur crée une valeur de hachage à sens unique qu'il envoie à la cible. La valeur de hachage contient trois éléments : une valeur d'ID prédéfinie, la valeur aléatoire que la cible envoie et une valeur privée, ou secret CHAP, que l'initiateur et la cible partagent. Lorsque la cible reçoit la valeur de hachage de l'initiateur, elle crée sa propre valeur de hachage en utilisant les mêmes éléments et la compare à la valeur de hachage de l'initiateur. Si les résultats correspondent, la cible authentifie l'initiateur.

ESXi prend en charge l'authentification CHAP unidirectionnelle et bidirectionnelle pour l'iSCSI. En authentification CHAP unidirectionnelle, la cible authentifie l'initiateur, mais l'initiateur n'authentifie pas la cible. En authentification CHAP bidirectionnelle, un niveau de sécurité supplémentaire permet à l'initiateur d'authentifier la cible.

ESXi prend en charge l'authentification CHAP au niveau de l'adaptateur, lorsqu'un seul jeu d'informations d'authentification peut être envoyé de l'hôte vers toutes les cibles. Il prend également en charge l'authentification CHAP par cible, qui vous permet de configurer des informations d'authentification différentes pour atteindre un perfectionnement plus important de la cible.

Reportez-vous à la documentation *Stockage vSphere* pour plus d'informations sur l'utilisation de CHAP.

Désactivation de l'authentification SAN iSCSI

Vous pouvez configurer le SAN iSCSI pour fonctionner sans authentification. Les communications entre l'initiateur et la cible sont toujours authentifiées de manière rudimentaire, car les périphériques cibles iSCSI sont généralement configurés pour communiquer avec des initiateurs spécifiques uniquement.

Choisir de ne pas imposer une authentification plus contraignante peut être pertinent si votre stockage iSCSI doit être hébergé à un seul emplacement et si vous devez créer un réseau dédié ou un VLAN pour prendre en charge tous vos périphériques iSCSI. La configuration iSCSI est sécurisée, car elle est isolée de tout accès non autorisé, tout comme un SAN Fibre Channel l'est.

En règle générale, désactivez l'authentification uniquement si vous souhaitez risquer une attaque au SAN iSCSI ou résoudre des problèmes provenant d'erreurs humaines.

Reportez-vous à la documentation *Stockage vSphere* pour plus d'informations sur l'utilisation de CHAP.

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.

Niveau de sécurité du chiffrement

La transmission de données via des connexions non sécurisées présente un risque, car des utilisateurs malveillants pourraient scanner les données lors de leur acheminement sur le réseau. Par mesure de sécurité, les composants réseau incluent généralement un chiffrement des données, afin qu'elles ne puissent pas être lues facilement.

Pour chiffrer les données, le composant expéditeur (passerelle ou composant de redirection, par exemple) applique des algorithmes (ou chiffrement) afin de modifier les données avant leur transmission. Le composant destinataire utilise une clé pour déchiffrer les données, qui reprennent leur forme d'origine. Plusieurs méthodes de chiffrement sont utilisées, qui offrent différents niveaux de sécurité. Pour mesurer la capacité d'un chiffrement à protéger les données, on peut utiliser le niveau de cryptage, qui représente le nombre d'octets présents dans la clé de chiffrement. Plus ce nombre est élevé, plus le chiffrement est sécurisé.

Pour garantir la protection des données transmises de et vers des connexions réseau externes, ESXi utilise l'un des chiffrements les plus sécurisés du marché : le chiffrement AES 256 bits. Pour les échanges de clés, ESXi utilise également la méthode RSA 1024 bits. Ces algorithmes de chiffrement sont utilisés par défaut pour les connexions suivantes.

- Connexions vSphere Client vers vCenter Server et vers ESXi via l'interface de gestion.
- Connexions SDK vers vCenter Server et vers ESXi.
- Connexions de l'interface de gestion vers les machines virtuelles via VMkernel.
- Connexions SSH vers ESXi, via l'interface de gestion.

Sécurité SSH

Vous pouvez utiliser SSH pour vous connecter à distance au Shell ESXi 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. Si cette configuration est trop restreinte, vous pouvez diminuer les valeurs affectées aux paramètres de sécurité.

Sécurisation de l'interface de gestion 3

La sécurité de l'interface de gestion ESXiest primordiale pour la protéger des intrusions et autorisations illégales.

Si un hôte est compromis de certaines façons, les machines virtuelles avec lesquelles il interagit peuvent l'être également. Pour minimiser le risque d'attaque via l'interface de gestion, ESXi est protégé au moyen d'un pare-feu.

Ce chapitre aborde les rubriques suivantes :

Recommandations générales de sécurité

Pour protéger l'hôte contre les intrusions et autorisations illégales, VMware impose des contraintes au niveau de plusieurs paramètres et activités. Vous pouvez les alléger en fonction de vos besoins de configuration ; toutefois, si vous le faites, assurez-vous que votre environnement est sécurisé et que vous avez pris toutes les autres mesures de sécurité requises pour protéger le réseau dans sa globalité, ainsi que les périphériques connectés à l'hôte.

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

- Limitez l'accès utilisateur.

  Pour augmenter la sécurité, limitez l'accès des utilisateurs à l'interface de gestion, et mettez en œuvre des règles de sécurité d'accès, comme des limitations de mots de passe.

  L'Shell ESXi possède un accès privilégié à certaines parties de l'hôte. Par conséquent, vous ne devez octroyer une autorisation d'accès à Shell ESXi qu'à certains utilisateurs de confiance.

  Vous ne devez également exécuter que les processus, services et agents essentiels (tels que les anti-virus et les sauvegardes de machine virtuelle).

- Utilisez vSphere Client pour gérer les hôtes ESXi.

  Utilisez dès que vous le pouvez vSphere Client, ou encore un outil de gestion de réseau tiers pour l'administration de vos hôtes ESXi et non l'interface de ligne de commande en tant qu'utilisateur racine. L'utilisation de vSphere Client permet de limiter le nombre de comptes ayant accès à Shell ESXi, de déléguer des responsabilités en toute sécurité et de configurer des rôles empêchant les administrateurs et les utilisateurs d'utiliser les fonctions dont ils n'ont pas besoin.

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

L'hôte utilise un grand nombre de produits tiers pour soutenir les interfaces de gestion ou les tâches de gestion à exécuter. VMware ne prend pas en charge la mise à niveau de ces produits s'ils ne proviennent pas 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. Visitez régulièrement les sites Web de fournisseurs tiers, ainsi que la base de connaissances VMware pour connaître les alertes de sécurité correspondantes.

Outre la mise en place du pare-feu, d'autres méthodes sont utilisées pour limiter les risques pour les hôtes :

- ESXi exécute uniquement les services nécessaires à la gestion de son fonctionnement, et la distribution est limitée aux fonctions requises pour l'exécution d'ESXi.
- Par défaut, tous les ports non requis pour la gestion des accès à l'hôte sont fermés. Vous devez ouvrir spécialement les ports associés aux services supplémentaires dont vous avez besoin.
- Par défaut, les chiffrements faibles sont désactivés, et toutes 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 sous ESXi utilisent SHA-1 avec chiffrement RSA en tant qu'algorithme de signature.
- Le service Web Tomcat, utilisé en interne par ESXi pour soutenir les accès des clients Web, a été modifié : il exécute uniquement les fonctions requises pour les tâches d'administration et de surveillance effectuées par un client Web. 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, en cas de besoin, envoie un correctif de sécurité.
- 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 ; par conséquent, il est conseillé de les privilégier et d'éviter d'utiliser les services non sécurisés. Si vous devez utiliser des services non sécurisés et que l'hôte bénéficie d'un niveau suffisant de sécurité, vous devez dans ce cas ouvrir les ports correspondants.

Remarque Suivez uniquement les instructions de sécurité fournies par VMware, disponible sur le site http://www.vmware.com/fr/technical-resources/virtualization-topics/security.

ESXi

ESXi contient un pare-feu situé entre l'interface de gestion et le réseau. Le pare-feu est activé par défaut.

Lors de l'installation, le pare-feu d'ESXi est configuré pour bloquer le trafic entrant et sortant, excepté le trafic des services par défaut répertoriés dans « Ports TCP et UDP pour l'accès de gestion », page 21.

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 ajouter des services pris en charge et des agents de gestion qui sont nécessaires à l'exécution de l'hôte en ajoutant des fichiers de configuration d'ensemble de règles au répertoire du pare-feu d'ESXi `/etc/vmware/firewall/`. Le fichier de configuration d'ensemble de règles par défaut est `service.xml`. Le fichier contient des règles de pare-feu et décrit la relation de chaque règle avec les ports et les protocoles.

Remarque 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 de l'ensemble de règles du client NFS », page 42 pour plus d'informations.

Fichiers de configuration d'ensemble de règles

Un fichier de configuration d'ensemble de règles contient des règles de pare-feu et décrit la relation de chaque règle avec les ports et les protocoles. Le fichier de configuration d'ensemble de règles peut contenir des ensembles de règles de plusieurs services.

Les fichiers de configuration d'ensemble de règles se trouvent dans le répertoire `/etc/vmware/firewall/`. Pour ajouter un service au profil de sécurité de l'hôte, vous devez définir les règles de port du service dans un fichier de configuration. Nommez le fichier de configuration *service_name*`.xml`.

Chaque ensemble de règles d'un service figurant dans un fichier de configuration d'ensemble de règles contient les informations suivantes.

- L'identifiant numérique du service, si le fichier de configuration contient plus d'un service.
- L'identifiant unique de l'ensemble de règles, généralement le nom du service.
- Pour chaque règle, le fichier contient une ou plusieurs règles de port, chacune comportant une définition de la direction, du protocole, du type de port et du numéro de port ou des numéros de plage de port.
- Une indication précisant si le service est activé ou désactivé lorsque l'ensemble de règles est appliqué.
- Une indication précisant si l'ensemble de règle est requis et s'il ne peut être désactivé.

Lorsque vous avez ajouté un service ou une règle au fichier de configuration, vous devez actualiser les paramètres du pare-feu.

Exemple : Fichier de configuration d'ensemble de règles

```
<ConfigRoot>
<service id='0000'>
 <id>serviceName</id>
  <rule id = '0000'>
   <direction>inbound</direction>
   <protocol>tcp</protocol>
   <porttype>dst</porttype>
   <port>80</port>
  </rule>
  <rule id='0001'>
   <direction>inbound</direction>
   <protocol>tcp</protocol>
   <porttype>src</porttype>
   <port>
    <begin>1020</begin>
    <end>1050</end>
   </port>
 </rule>
 <enabled>true</enabled>
    <required>false</required>
</service>
</ConfigRoot>
```

Ajouter un ensemble de règles au pare-feu ESXi

Un ensemble de règles décrit les règles de port d'un service.

Les fichiers de configuration doivent être installés à l'aide d'un module VIB. Lorsque vous incluez un fichier de configuration d'ensemble de règles à un module VIB et utilisez le chemin d'installation `/etc/vmware/firewall/`, le système détecte le fichier et actualise le pare-feu automatiquement.

Procédure

1 À l'aide d'un éditeur de texte, créez un fichier de configuration.

Option	Description
<service id='*nnnn*'>	Identifiant numérique du service. Si le fichier de configuration ne contient qu'un seul service, vous n'avez pas besoin d'ID de service. Utilisez `<service></service>`.
<id>	Généralement le nom du service.
<rule id='*nnnn*'>	Identifiant numérique de la règle.
<direction>	Direction du port (entrant ou sortant).
<protocol>	Protocole du port (tcp ou udp).
<porttype>	Type de port : source ou de destination (src ou dst).
<port>	Numéro de port ou plage de ports. Pour entrer une plage, utilisez les balises <begin> et <end>.
<enabled>	Statut du service lorsque l'ensemble de règles est appliqué (vrai ou faux).
<required>	Indique si l'ensemble de règle est requis et s'il ne peut être désactivé (vrai ou faux).

2 Enregistrez le fichier sous le nom *service_name*`.xml`.

Exemple : Fichier de configuration d'ensemble de règles

```
<ConfigRoot>
<service id='0016'>
 <id>webAccess</id>
  <rule id='0000'>
   <direction>inbound</direction>
   <protocol>tcp</protocol>
   <porttype>dst</porttype>
   <port>80</port>
  </rule>
     <rule id='0001'>
   <direction>inbound</direction>
   <protocol>tcp</protocol>
   <porttype>src</porttype>
   <port>
    <begin>1020</begin>
    <end>1050</end>
   </port>
  </rule>
 <enabled>true</enabled>
 <required>true</required>
</service>
</ConfigRoot>
```

Suivant

Lorsque vous installez un module VIB, le fichier est automatiquement chargé et vous n'avez pas besoin d'actualiser le pare-feu. Si vous ajoutez directement un fichier de configuration d'ensemble de règles à `/etc/vmware/firewall/`, vous devez actualiser le pare-feu manuellement.

Appliquer ou actualiser l'ensemble de règles de pare-feu

Une fois que vous avez ajouté ou modifié un ensemble de règles de pare-feu, vous devez actualiser le pare-feu pour charger la nouvelle règle.

Dans la procédure, `--server=server_name` spécifie le serveur cible. Le serveur cible spécifié vous invite à saisir un nom de serveur et un mot de passe. D'autres options de connexion, telles qu'un fichier de configuration ou de session, sont prises en charge. Pour obtenir une liste des options de connexion, reportez-vous à *Initiation aux interfaces de ligne de commande vSphere*.

Prérequis

Créez un fichier de configuration d'ensemble de règles et ajoutez-y les règles de pare-feu.

Installez vCLI ou déployez la machine virtuelle de vSphere Management Assistant (vMA). Reportez-vous à la section *Initiation aux interfaces de ligne de commande vSphere*. Pour le dépannage, exécutez les commandes `esxcli` dans ESXi Shell.

Procédure

- Sur l'invite de commande, chargez tous les fichiers de configuration mis à jour en exécutant la commande suivante :

  ```
  esxcli --server=server_name network firewall refresh
  ```

Le cache de l'agent hôte est mis à jour avec les dernières informations de configuration de pare-feu.

Autoriser ou refuser l'accès à un service ESXi ou à un agent de gestion

Vous pouvez configurer les propriétés du pare-feu pour autoriser ou refuser l'accès à un service ou un agent de gestion.

Vous ajoutez des informations sur les services et agents de gestion autorisés dans le fichier de configuration de l'hôte. Vous pouvez activer ou désactiver ces services et agents à l'aide de vSphere Client ou de la ligne de commande.

Remarque Si les différents services ont des règles de port qui se chevauchent, l'activation d'un service pourra implicitement autoriser les services se chevauchant. Afin de minimiser les effets de ce comportement, vous pouvez spécifier les adresses IP autorisées à accéder à chaque service sur l'hôte.

Procédure

1. Connectez-vous à un système vCenter Server en utilisant vSphere Client.
2. Sélectionnez l'hôte dans le panneau d'inventaire.
3. Cliquez sur l'onglet **[Configuration]** , puis cliquez sur **[Profil de sécurité]** .

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

   La boîte de dialogue Propriétés de pare-feu énumère tous les ensembles de règles que vous pouvez configurer pour l'hôte.
5. Sélectionnez les ensembles de règles à activer, ou désélectionnez ceux à désactiver.

   Les colonnes Ports entrants et Ports sortants indiquent les ports que vSphere Client ouvre pour le service. La colonne Protocole indique le protocole que le service utilise. La colonne Démon indique le statut des démons associés au service.
6. Cliquez sur **[OK]** .

Comportement de l'ensemble de règles du client NFS

Le comportement de l'ensemble de règles du client NFS diffère de celui des autres ensembles de règles du pare-feu d'ESXi. ESXi configure les paramètres du client NFS lorsque vous montez ou démontez une banque de données NFS.

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

- Si l'ensemble de règles du client NFS est désactivé, ESXi l'active et désactive Autorisez la règle Toutes les adresses IP en paramétrant l'indicateur `allowedAll` sur `FAUX`. L'adresse IP du serveur NFS est ajoutée à la liste des adresses IP sortantes autorisées.
- Si l'ensemble de règles du client NFS est activé, l'état de l'ensemble de règles et la règle des adresses IP ne sont pas modifiés. L'adresse IP du serveur NFS est ajoutée à la liste des adresses IP sortantes autorisées.

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

- Si ESXi est monté sur une banque de données NFS, l'adresse IP du serveur NFS démonté est supprimée de la liste des adresses IP sortantes autorisées et l'ensemble de règles du client NFS reste activé.
- Si ESXi n'est pas monté sur une banque de données NFS, l'adresse IP du serveur NFS démonté est supprimée de la liste des adresses IP sortantes autorisées et l'ensemble de règles du client NFS est désactivé.

Remarque Si vous activez manuellement l'ensemble de règles du client NFS ou configurez manuellement la règle Toutes les adresses IP, que ce soit avant ou après l'ajout d'une banque de données NFS sur le système, vos paramètres sont remplacés lorsque la dernière banque de données NFS est démontée. L'ensemble de règle du client NFS est désactivé lorsque toutes les banques de données NFS sont démontées.

Ajouter des adresses IP autorisées

Vous pouvez spécifier les réseaux qui sont autorisés à se connecter à chaque service exécuté sur l'hôte.

Vous pouvez utiliser vSphere Client ou la ligne de commande pour mettre à niveau la liste des adresses IP autorisées d'un service. Par défaut, toutes les adresses IP sont autorisées.

Procédure

1. Connectez-vous à un système vCenter Server en utilisant vSphere Client.
2. Sélectionnez l'hôte dans le panneau d'inventaire.
3. Cliquez sur l'onglet **[Configuration]** , puis cliquez sur **[Profil de sécurité]** .
4. Dans la section Pare-feu, cliquez sur **[Propriétés]** .
5. Sélectionnez un service dans la liste et cliquez sur **[Pare-feu]** .
6. Sélectionnez **[Autoriser uniquement les connexions depuis les réseaux suivants]** et entrez les adresses IP des réseaux autorisés à se connecter à l'hôte.

   Vous pouvez entrer les adresses IP dans les formats suivants : 192.168.0.0/24, 192.168.1.2, 2001::1/64 ou fd3e:29a6:0a81:e478::/64.
7. Cliquez sur **[OK]** .

Automatisation du comportement du service en fonction des paramètres du pare-feu

ESXi peut automatiser le démarrage des services en fonction de l'état des ports du pare-feu.

L'automatisation permet de garantir que les services démarrent si l'environnement est configuré pour activer leur fonction. Par exemple, le démarrage d'un service réseau uniquement lorsque certains ports sont ouverts permet d'éviter des situations dans lesquelles les services sont démarrés, mais incapables de terminer les communications requises pour remplir l'objectif prévu.

Par ailleurs, disposer d'informations précises sur l'heure actuelle est une contrainte pour certains protocoles, tels que Kerberos. Le service NTP permet d'obtenir des informations d'heure précise, mais ce service fonctionne uniquement lorsque les ports requis sont ouverts sur le pare-feu. Ce service ne peut pas remplir cet objectif si tous les ports sont fermés. Les services NTP permettent de configurer les conditions de démarrage et d'arrêt du service. Cette configuration comprend des options qui vérifient que les ports du pare-feu sont ouverts, puis démarrent ou arrêtent le service NTP en fonction de ces conditions. Plusieurs options de configuration possible existent, celles-ci étant toutes applicables au serveur SSH.

Remarque Les paramètres décrits dans cette section s'appliquent uniquement aux paramètres de service configurés via vSphere Client ou des applications créées avec le SDK des services Web vSphere. Les configurations effectuées avec d'autres méthodes, telles que l'Shell ESXi ou les fichiers de configuration se trouvant dans `/etc/init.d/`, ne se trouvent pas affectées par ces paramètres.

- **[Commencez automatiquement si des ports sont ouverts, et arrêtez lorsque tous les ports sont fermés]** : Les paramètres par défaut de ces services que VMware recommande. Si un port est ouvert, le client tente de contacter les ressources réseau correspondant au service en question. Si certains ports sont ouverts, mais que le port d'un service particulier est fermé, la tentative échoue, mais un tel cas pose peu d'inconvénient. Si et lorsque le port de sortie applicable est ouvert, le service commence à effectuer sa tâche.
- **[Commencez et arrêtez avec l'hôte]** : Le service démarre peu après le démarrage de l'hôte et se ferme 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 préserve les paramètres de service déterminés par l'utilisateur, quels que soient les ports 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 Le pare-feu d'ESXi automatise l'activation et la désactivation des ensembles de règles selon la règle de démarrage des services. Lorsqu'un service démarre, l'ensemble de règle lui correspondant est activé. Lorsque le service s'arrête, l'ensemble de règles est désactivé.

Définir le Service ou les options de démarrage de client

Par défaut, les processus du démon commencent lorsqu'un de leurs ports est ouvert et s'arrêtent lorsque tous les ports sont fermés. Vous pouvez changer cette règle de démarrage pour le service ou le client sélectionné.

Procédure

1. Connectez-vous à un système vCenter Server en utilisant vSphere Client.
2. Sélectionnez l'hôte dans le panneau d'inventaire.
3. Cliquez sur l'onglet **[Configuration]** , puis cliquez sur **[Profil de sécurité]** .

4 Dans la section Pare-feu, cliquez sur **[Propriétés]** .

La boîte de dialogue Propriétés de pare-feu énumère tous les services et agents de gestion que vous pouvez configurer pour l'hôte.

5 Sélectionnez le service ou l'agent de gestion à configurer et cliquez sur **[Options]** .

La boîte de dialogue Startup Policy détermine le moment auquel le service démarre. Cette boîte de dialogue fournit des informations sur l'état actuel du service et une interface pour démarrer, arrêter ou redémarrer manuellement le service.

6 Sélectionnez une stratégie dans la liste **[Règle démarrage]** .

7 Cliquez sur **[OK]** .

ESXi

Vous pouvez configurer le pare-feu d'ESXi dans l'invite de commande.

Configuration du pare-feu à l'aide du ESXi Shell

L'interface utilisateur graphique de vSphere Client indique les modes d'exécution privilégiés de nombreuses tâches de configuration. Cependant, vous pouvez utiliser le Shell ESXi pour configurer ESXi dans l'invite de commande si nécessaire.

Tableau 3-1. Commandes du pare-feu

Commande	Description
`esxcli network firewall get`	Renvoie le statut activé ou désactivé du pare-feu et énumère les actions par défaut.
`esxcli network firewall set --defaultaction`	mettre à niveau les actions 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 --allowedall`	Configurer l'indicateur `allowedall`.
`esxcli network firewall ruleset set --enabled`	Activer ou désactiver l'ensemble de règles spécifié.
`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.

Authentification et gestion d'utilisateurs

4

ESXi gère l'authentification des utilisateurs et prend en charge les autorisations de groupes et d'utilisateurs. Par ailleurs, vous pouvez chiffrer des connexions à SDK et au vSphere Client.

Ce chapitre aborde les rubriques suivantes :

Sécuriser ESXi via l'authentification et les autorisations

Lorsqu'un utilisateur de vSphere Client ou de vCenter Server se connecte à ESXi, une connexion est établie avec le processus d'agent hôte de VMware. Le processus se sert des mots de passe et noms d'utilisateur pour effectuer une authentification.

ESXi authentifie les utilisateurs qui accèdent aux hôtes à l'aide de SDK ou de vSphere Client. L'installation par défaut d'ESXi utilise une base de données de mots de passe locale pour l'authentification.

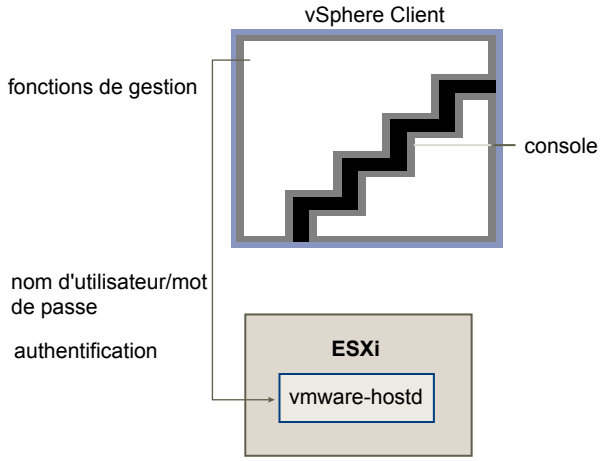
ESXi utilise la structure PAM (Pluggable Authentication Modules) pour effectuer une authentification quand les utilisateurs accèdent à l'hôte ESXi via vSphere Client. La configuration PAM pour les services VMware se trouve dans `/etc/pam.d/system-auth-generic` où sont stockés les chemins d'accès aux modules d'authentification. La modification de cette configuration affecte tous les services des hôtes.

Le proxy inverse dans le processus d'agent hôte de VMware écoute sur les ports 80 et 443. Les utilisateurs de vSphere Client ou de vCenter Server se connectent à l'agent hôte via ces ports. Le processus de l'hôte reçoit le mot de passe et nom d'utilisateur depuis le client et les transmet au module PAM afin d'effectuer l'authentification.

La figure qui suit montre un exemple basique d'authentification des transactions par l'hôte depuis vSphere Client.

Remarque Les transactions CIM utilisent également l'authentification par ticket en se connectant avec le processus de l'hôte.

Figure 4-1. Authentification des communications de vSphere Client avec ESXi



Pour garantir que l'authentification fonctionne efficacement pour votre site, effectuez des tâches basiques telles que la configuration d'utilisateurs, groupes, autorisations et rôles, la configuration d'attributs utilisateurs, l'ajout de vos propres certificats et l'utilisation éventuelle de SSL.

Gestion des utilisateurs de vSphere

Un utilisateur est un individu autorisé à ouvrir une session sur ESXi ou sur vCenter Server.

Les utilisateurs ESXi entrent dans deux catégories : ceux qui peuvent accéder à l'hôte via vCenter Server et ceux qui peuvent y accéder en ouvrant directement une session de l'hôte depuis le vSphere Client, un client tiers, ou une invite de commande.

Utilisateurs de vCenter Server autorisés

Les utilisateurs autorisés pour vCenter Server sont ceux inclus dans la liste de domaine Windows référencée par vCenter Server ou la liste d'utilisateurs locaux de Windows dans l'hôte vCenter Server.

Vous ne pouvez pas utiliser vCenter Server pour créer, supprimer ou modifier manuellement des utilisateurs. Vous devez utiliser les outils pour gérer votre domaine Windows. Les changements que vous effectuez s'appliquent à vCenter Server. Toutefois, l'interface utilisateur ne vous fournit pas de liste d'utilisateurs à passer en revue.

Utilisateurs à accès direct

Les utilisateurs autorisés à travailler directement sur l'hôte sont ajoutés à la liste d'utilisateurs internes par un administrateur système.

Un administrateur peut effectuer plusieurs activités de gestion pour ces utilisateurs, comme par exemple modifier les mots de passe, les adhésions aux groupes, les autorisations, ou encore ajouter et supprimer des utilisateurs.

La liste d'utilisateurs que ESXi gère localement se distingue des utilisateurs connus par vCenter Server, ces derniers étant des utilisateurs Windows locaux ou faisant partie du domaine Windows. Si l'authentification Active Directory a été configurée sur l'hôte, les mêmes utilisateurs du domaine Windows connus par vCenter Server seront disponibles sur l'hôte ESXi.

Meilleures pratiques pour les utilisateurs de vSphere

Utilisez les meilleures pratiques pour créer et gérer les utilisateurs afin d'augmenter la sécurité et la gérabilité de votre environnement vSphere.

VMware recommande plusieurs meilleures pratiques pour créer des utilisateurs dans votre environnement vSphere :

- Ne créez pas d'utilisateur **ALL**. Les privilèges associés au nom **ALL** peuvent ne pas être disponibles pour tous les utilisateurs dans certains cas. Par exemple, si l'utilisateur **ALL** a les privilèges d'adminsitrateur, un utilisateur avec les privilièges **ReadOnly** peut se connecter à distance à l'hôte, ce qui n'est pas le comportement désiré.
- Utilisez un service d'annuaire ou vCenter Server pour centraliser le contrôle d'accès, plutôt que de définir des utilisateurs sur des hôtes individuels.
- Choisissez un utilisateur ou un groupe local Windows comme ayant le rôle d'administrateur dans vCenter Server.
- En raison de la confusion causée par les noms doubles, contrôlez la liste d'utilisateurs vCenter Server avant de créer des utilisateurs de l'hôte ESXi pour éviter les doublons. Pour contrôler les utilisateurs de vCenter Server, consultez la liste de domaine Windows.

Important Par défaut, certaines versions du système d'exploitation Windows comprennent l'utilisateur NT AUTHORITY\INTERACTIVE dans le groupe d'administrateurs. Lorsque l'utilisateur NT AUTHORITY\INTERACTIVE se trouve dans le groupe d'administrateurs, tous les utilisateurs que vous créez sur le système vCenter Server ont le privilège Administrateur. Pour éviter cela, supprimez l'utilisateur NT AUTHORITY\INTERACTIVE du groupe d'administrateurs du système Windows où vous exécutez vCenter Server.

Ajouter un utilisateur local

Ajouter un utilisateur au tableau d'utilisateurs met à jour la liste d'utilisateurs interne conservée par l'hôte.

Prérequis

Passez en revue les exigences de mot de passe décrites dans « Exigences de mots de passe », page 52.

Procédure

1. Connectez-vous à ESXi en utilisant vSphere Client.
2. Cliquez sur l'onglet **[Utilisateurs et groupes locaux]** et sur **[Utilisateurs]** .
3. Cliquez avec le bouton droit n'importe où dans le tableau d'utilisateurs, puis cliquez sur **[Ajouter]** pour ouvrir la boîte de dialogue Ajouter un nouvel utilisateur.
4. Saisissez un identifiant, un nom d'utilisateur, un ID d'utilisateur numérique (UID) et un mot de passe.

   Remarque Ne créez pas d'utilisateur **ALL**. Les privilèges associés au nom **ALL** peuvent ne pas être disponibles pour tous les utilisateurs dans certains cas. Par exemple, si l'utilisateur **ALL** a les privilèges d'adminsitrateur, un utilisateur avec les privilièges **ReadOnly** peut se connecter à distance à l'hôte, ce qui n'est pas le comportement désiré.

   - La saisie du nom d'utilisateur et de l'UID est facultative. Si vous n'indiquez pas d'UID, le vSphere Client attribue le prochain UID disponible.

- Créez un mot de passe qui répond aux exigences de longueur et de complexité. L'hôte contrôle la conformité du mot de passe à l'aide du plug-in d'authentification par défaut, `pam_passwdqc.so`. Si le mot de passe n'est pas conforme, l'erreur suivante s'affiche : `Une erreur générale du système s'est produite : mot de passe : Erreur de manipulation de jeton d'authentification`.

5 Pour changer les droits d'accès à ESXi de l'utilisateur via un shell de commande, sélectionnez ou désélectionnez **[Octroi accès shell à cet utilisateur]** .

Remarque Pour être autorisé à accéder au shell, les utilisateurs doivent aussi avoir un rôle Administrateur pour un objet d'inventaire sur l'hôte.

En général, n'accordez pas l'accès au shell à moins que l'utilisateur en ait un besoin justifié. Les utilisateurs qui accèdent uniquement à l'hôte via le vSphere Client n'ont pas besoin d'accéder au shell.

6 Pour ajouter l'utilisateur à un groupe, sélectionnez le nom du groupes dans le menu déroulant **[groupes]** , puis cliquez sur **[Ajouter]** .

7 Cliquez sur **[OK]** .

Modifier les paramètres pour un utilisateur sur l'hôte

Vous pouvez modifier l'ID utilisateur, le nom d'utilisateur, le mot de passe et les paramètres de groupes d'un utilisateur. Vous pouvez également accorder l'accès shell à l'utilisateur.

Prérequis

Passez en revue les exigences de mot de passe décrites dans « Exigences de mots de passe », page 52.

Procédure

1 Connectez-vous à ESXi en utilisant vSphere Client.

2 Cliquez sur l'onglet **[Utilisateurs et groupes locaux]** et sur **[Utilisateurs]** .

3 Cliquez avec le bouton droit sur l'utilisateur, puis cliquez sur **[Modifier]** pour ouvrir la boîte de dialogue Modifier l'utilisateur.

4 Pour modifier l'ID de l'utilisateur, saisissez un UID d'utilisateur numérique dans la zone de texte **[UID]** .

vSphere Client assigne l'UID lorsque vous créez l'utilisateur pour la première fois. Dans la plupart des cas, vous ne devez pas modifier cette attribution.

5 Entrer un nouveau nom d'utilisateur.

6 Pour changer le mot de passe de l'utilisateur, sélectionnez **[Changer mot de passe]** et entrez le nouveau mot de passe.

Créez un mot de passe qui répond aux exigences de longueur et de complexité. L'hôte contrôle la conformité du mot de passe à l'aide du plug-in d'authentification par défaut, `pam_passwdqc.so`. Si le mot de passe n'est pas conforme, l'erreur suivante s'affiche : `Une erreur générale du système s'est produite : mot de passe : Erreur de manipulation de jeton d'authentification`.

7 Pour changer les droits d'accès à ESXi de l'utilisateur via un shell de commande, sélectionnez ou désélectionnez **[Octroi accès shell à cet utilisateur]** .

Remarque Pour être autorisé à accéder au shell, les utilisateurs doivent aussi avoir un rôle Administrateur pour un objet d'inventaire sur l'hôte.

En général, n'accordez pas l'accès au shell à moins que l'utilisateur en ait un besoin justifié. Les utilisateurs qui accèdent uniquement à l'hôte via le vSphere Client n'ont pas besoin d'accéder au shell.

8 Pour ajouter l'utilisateur à un groupe, sélectionnez le nom du groupes dans le menu déroulant **[groupes]** , puis cliquez sur **[Ajouter]** .

9 Pour supprimer l'utilisateur d'un groupe, sélectionnez le nom du groupe dans la boîte **[Appartenance groupes]** et cliquez sur **[Supprimer]** .

10 Cliquez sur **[OK]** .

Supprimer un utilisateur de l'hôte

Vous pouvez supprimer un utilisateur de l'hôte.

Avertissement Ne retirez pas l'utilisateur racine.

Si vous supprimez un utilisateur de l'hôte, il perd les autorisations sur tous les objets de l'hôte et ne peut plus ouvrir une session.

Remarque Les utilisateurs qui ont ouvert une session et sont supprimés du domaine gardent leurs autorisations hôtes jusqu'au redémarrage de l'hôte.

Procédure

1 Connectez-vous à ESXi en utilisant vSphere Client.

2 Cliquez sur l'onglet **[Utilisateurs et groupes locaux]** et sur **[Utilisateurs]** .

3 Cliquez avec le bouton droit sur l'utilisateur à supprimer et sélectionnez **[Supprimer]** .

En aucun cas ne retirez l'utilisateur racine.

Supprimer ou modifier des utilisateurs de vCenter Server

Quand vous supprimez des utilisateurs de vCenter Server, vous enlevez également les autorisations accordées à ces utilisateurs. La modification d'un nom d'utilisateur ou de groupe rend le nom initial incorrect.

Pour supprimer des utilisateurs de vCenter Server, vous devez les supprimer du domaine ou de la liste d'utilisateurs d'Active Directory.

Si vous supprimez des utilisateurs du domaine de vCenter Server, ils perdent les autorisations sur tous les objets dans l'environnement vSphere et ne peuvent pas ouvrir à nouveau une session.

Remarque Les utilisateurs qui ont ouvert une session et sont supprimés du domaine gardent leurs autorisations de vSphere jusqu'à la période suivante de validation. La période par défaut est toutes les 24 heures.

La suppression d'un groupe n'affecte pas les autorisations accordées individuellement aux utilisateurs de ce groupes ou les autorisations accordées en tant qu'élément d'inclusion à un autre groupe.

Si vous changez un nom d'utilisateur dans le domaine, alors le nom d'utilisateur initial n'est plus valide dans le système de vCenter Server. Si vous changez le nom d'un groupe, le groupe initial devient incorrect après le redémarrage du système vCenter Server.

Trier, exporter et afficher les utilisateurs et les groupes

Vous pouvez afficher, trier et exporter des listes d'utilisateurs et de groupes dans un fichier au format HTML, XML, Microsoft Excel ou CSV.

Procédure

1 Connectez-vous à ESXi en utilisant vSphere Client.

2 Cliquez sur l'onglet **[Utilisateurs et groupes locaux]** , puis sur **[Utilisateurs]** ou **[Groupes]** .

3 Décidez comment vous voulez trier le tableau, puis masquez ou affichez les colonnes selon l'information que vous souhaitez voir dans le fichier exporté.
   - Pour trier le tableau par n'importe quelle colonne, cliquez sur l'en-tête de colonne.
   - Pour afficher ou masquer les colonnes, cliquez avec le bouton droit sur les en-têtes de colonne et sélectionnez ou désélectionnez le nom de la colonne à masquer.
   - Pour afficher ou masquer les colonnes, cliquez avec le bouton droit sur les en-têtes de colonne et sélectionnez ou désélectionnez le nom de la colonne à masquer.
4 Cliquez avec le bouton droit n'importe où dans le tableau, puis cliquez sur **[Exporter liste]** pour ouvrir la boîte de dialogue Enregistrer sous.
5 Sélectionnez un chemin d'accès et entrez un nom de fichier.
6 Sélectionnez le type de fichier, puis cliquez sur **[OK]** .

Gestion des groupes de vSphere

Un groupe est un ensemble d'utilisateurs partageant plusieurs règles et autorisations. Lorsque vous assignez des autorisations à un groupe, tous les utilisateurs du groupes en héritent, et vous n'êtes pas obligé d'utiliser les profils d'utilisateurs individuellement.

Les listes de groupes dans vCenter Server et l'hôte ESXi sont issues des mêmes sources que les listes de leurs utilisateurs respectifs. Les listes de groupes dans vCenter Server proviennent de la liste utilisateurs locaux ou d'un quelconque domaine approuvé, et les listes de groupes pour un hôte proviennent de la liste d'utilisateurs locaux ou de tout domaine Windows approuvé.

En tant qu'administrateur, choisissez comment structurer les groupes afin d'atteindre vos objectifs de sécurité et d'utilisation. Par exemple, trois membres de l'équipe commerciale travaillent à mi-temps à des jours différents, et vous souhaitez qu'ils partagent une machine virtuelle unique mais qu'ils n'utilisent pas les machines virtuelles appartenant aux directeurs commerciaux. Dans ce cas, vous pouvez créer un groupe appelé SalesShare incluant les trois membres de l'équipe et donner l'autorisation de groupes afin d'interagir avec un seul objet, la machine virtuelle partagée. Ils ne peuvent effectuer aucune action sur les machines virtuelles des directeurs commerciaux.

Meilleures pratiques pour les groupes de vSphere

Utilisez les meilleures pratiques pour gérer les groupes afin d'augmenter la sécurité et la gérabilité de votre environnement vSphere.

VMware recommande plusieurs meilleures pratiques pour créer des groupes dans votre environnement vSphere :

- Utilisez un service d'annuaire ou vCenter Server pour centraliser le contrôle d'accès, plutôt que de définir des groupes sur des hôtes individuels.
- Choisissez un utilisateur ou un groupe local Windows comme ayant le rôle d'administrateur dans vCenter Server.
- Créez de nouveaux groupes pour les utilisateurs de vCenter Server. Évitez d'utiliser les groupes intégrés ou les autres groupes existants Windows.

- Si vous utilisez des groupes d'Active Directory, assurez-vous qu'il s'agit de groupes de sécurité et pas de groupes de distribution.. Les autorisations assignées aux groupes de distribution ne sont pas appliquées par vCenter Server. Pour plus d'informations sur les groupes de sécurité et les groupes de distribution, consultez la documentation d'Active Directory de Microsoft .

Important Par défaut, certaines versions du système d'exploitation Windows comprennent l'utilisateur NT AUTHORITY\INTERACTIVE dans le groupe d'administrateurs. Lorsque l'utilisateur NT AUTHORITY\INTERACTIVE se trouve dans le groupe d'administrateurs, tous les utilisateurs que vous créez sur le système vCenter Server ont le privilège Administrateur. Pour éviter cela, supprimez l'utilisateur NT AUTHORITY\INTERACTIVE du groupe d'administrateurs du système Windows où vous exécutez vCenter Server.

Ajouter un groupe

Ajouter un groupe au tableau de groupes met à jour la liste de groupes interne conservée par l'hôte.

Procédure

1. Connectez-vous à ESXi en utilisant vSphere Client.
2. Cliquez sur **[Utilisateurs et groupes locaux]** et sur **[Groupes]** .
3. Cliquez avec le bouton droit n'importe où dans le tableau de groupes, puis cliquez sur **[Ajouter]** pour ouvrir la boîte de dialogue Créer un nouveau groupes.
4. Entrez le nom du groupe et un ID de groupe numérique (GID).

   La saisie de l'ID est facultative. Si vous ne spécifiez pas d'ID, vSphere Client attribue le prochain ID de groupe disponible.
5. Dans la liste des utilisateurs, sélectionnez l'utilisateur à ajouter et cliquez sur **[Ajouter]** .
6. Cliquez sur **[OK]** .

Supprimer un groupe d'un hôte

Vous pouvez supprimer un groupe de l'hôte.

La suppression d'un groupe n'affecte pas les autorisations accordées individuellement aux utilisateurs de ce groupes ou les autorisations accordées en tant qu'élément d'inclusion à un autre groupe.

Procédure

1. Connectez-vous à ESXi en utilisant vSphere Client.
2. Cliquez sur **[Utilisateurs et groupes locaux]** et sur **[Groupes]** .
3. Cliquez avec le bouton droit sur le groupe à supprimer et sélectionnez **[Supprimer]** .

Ajouter ou supprimer des utilisateurs d'un groupe

Vous pouvez ajouter ou supprimer un utilisateur d'un groupe du tableau de groupes.

Procédure

1. Connectez-vous à ESXi en utilisant vSphere Client.
2. Cliquez sur **[Utilisateurs et groupes locaux]** et sur **[Groupes]** .
3. Cliquez avec le bouton droit sur le groupes à modifier et sélectionnez **[Propriétés]** pour ouvrir la boîte de dialogue Modifier le groupes.
4. Pour ajouter l'utilisateur à un groupe, sélectionnez le nom de l'utilisateur dans le menu déroulant **[Utilisateur]** , puis cliquez sur **[Ajouter]** .

5 Pour supprimer l'utilisateur d'un groupe, sélectionnez le nom de l'utilisateur dans la boîte **[Utilisateurs de ce groupe]** et cliquez sur **[Supprimer]** .

6 Cliquez sur **[OK]** .

Exigences de mots de passe

Par défaut, ESXi applique des conditions pour les mots de passe utilisateur.

Lorsque vous créez un mot de passe, composez-le d'un mélange de caractères de quatre classes différentes : des lettres minuscules, des lettres majuscules, des chiffres et des caractères spéciaux tels qu'un caractère de soulignement ou un tiret.

Votre mot de passe doit être conforme aux conditions de longueur suivantes.

- Le mot de passe comportant des caractères d'une ou deux classes doit contenir au moins huit caractères.
- Le mot de passe comportant des caractères de trois classes doit contenir au moins sept caractères.
- Le mot de passe comportant des caractères des quatre classes doit contenir au moins six caractères.

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.

Vous pouvez aussi vous servir d'une phrase de passe, qui est une phrase composée d'au moins trois mots, ayant une longueur de 8 à 40 caractères chacun.

Exemple : Créer des mots de passe acceptables

Les candidats de mot de passe suivants répondent aux exigences d'ESXi.

- xQaTEhbU : Contient huit caractères provenant de deux classes de caractères.
- xQaT3pb : Contient sept caractères provenant de trois classes de caractères.
- xQaT3# : Contient six caractères provenant de quatre classes de caractères.

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

- Xqat3hb : Commence par un caractère majuscule, réduisant ainsi le nombre effectif de classes de caractères à deux. Huit caractères sont nécessaires lorsque vous n'utilisez que deux classes de caractères.
- xQaTEh2 : Se termine par un chiffre, réduisant ainsi le nombre effectif de classes de caractères à deux. Huit caractères sont nécessaires lorsque vous n'utilisez que deux classes de caractères.

Assignation d'autorisations

Pour ESXi et vCenter Server, les autorisations sont définies en tant que rôles d'accès et sont constituées d'un utilisateur et du rôle assigné à l'utilisateur pour un objet, tel qu'une machine virtuelle ou un hôte ESXi. Les autorisations accordent aux utilisateurs le droit d'exercer les activités spécifiées par le rôle sur l'objet auquel le rôle est assigné.

Par exemple, pour configurer la mémoire pour l'hôte, il faut accorder à l'utilisateur un rôle qui inclut le privilège **Hôte.Configuration.Configuration de mémoire** . En assignant différents rôles aux utilisateurs ou aux groupes pour différents objets, vous pouvez contrôler les tâches que les utilisateurs peuvent effectuer dans votre environnement vSphere.

Par défaut, tous les utilisateurs qui sont membres du groupe d'administrateurs de Windows sur le système vCenter Server ont les mêmes droits d'accès que ceux attribués à un utilisateur assigné au rôle d'administrateur sur tous les objets. En se connectant directement à l'hôte, les comptes d'utilisateur racine et vpxuser ont les mêmes droits d'accès que ceux assignés à tout utilisateur assigné au rôle d'administrateur sur tous les objets.

Tous les autres utilisateurs n'ont au commencement aucune autorisation sur aucun objet, ce qui signifie qu'ils ne peuvent pas consulter ces objets ou effectuer des opérations sur eux. Un utilisateur avec des privilèges d'administrateur doit assigner des autorisations à ces utilisateurs afin de leur permettre d'effectuer des tâches.

Beaucoup de tâches exigent des autorisations sur plus d'un objet. Ces règles peuvent vous aider à déterminer où vous devez assigner des autorisations pour autoriser des opérations spécifiques :

- 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. Déployer une machine virtuelle directement à un hôte ou à un cluster exige le privilège **Ressource.Attribuer une machine virtuelle au pool de ressources** .

La liste de privilèges est la même pour ESXi et vCenter Server, et vous utilisez la même méthode pour configurer des autorisations.

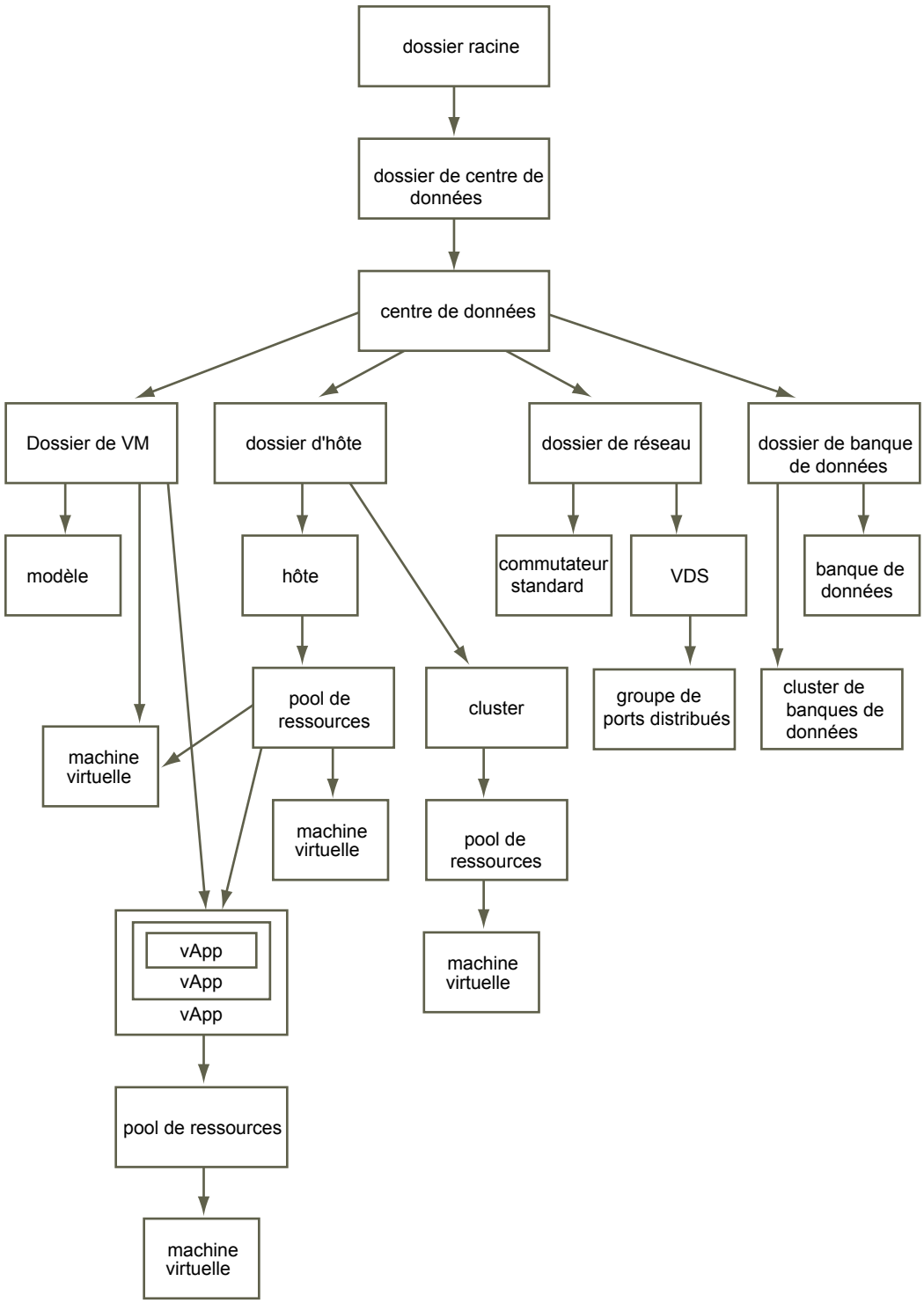
Vous pouvez créer des rôles et configurer des autorisations via une connexion directe à l'hôte ESXi.

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.

Figure 4-2. 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. Pour limiter les privilèges d'un utilisateur sur une machine virtuelle, vous devez définir des autorisations sur le dossier parent et l'hôte parent, le cluster, ou le pool de ressources parent de cette machine virtuelle.

Pour définir des autorisations pour un commutateur distribué et ses groupes de ports distribués associés, définissez les autorisations sur un objet parent, tel qu'un dossier ou le 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

Vous pouvez 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

Les entités globales dérivent des autorisations du système de 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.

Les autorisations appliquées sur un objet enfant ignorent toujours les autorisations qui sont appliquées sur un objet parent. Les dossiers et les pools de ressources de machine virtuelle ont des niveaux équivalents dans la hiérarchie. Si vous assignez une propagation des autorisations à un utilisateur ou à un groupe sur le dossier d'une machine virtuelle et son pool de ressources, l'utilisateur a les privilèges propagés du pool de ressources et du dossier.

Si des autorisations multiples de groupes sont définies sur le même objet et que l'utilisateur appartient à deux ou à plusieurs 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

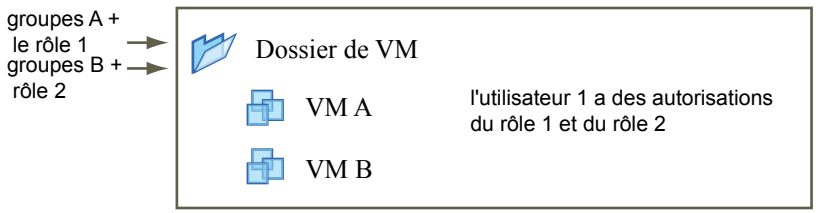
Cet exemple illustre comment un objet peut hériter d'autorisations multiples de groupes auxquels ont été accordés l'autorisation sur un objet parent.

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.
- L'utilisateur 1 ne dispose pas d'affectation d'autorisation spécifique.

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 4-3. Exemple 1 : Héritage d'autorisations multiples



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

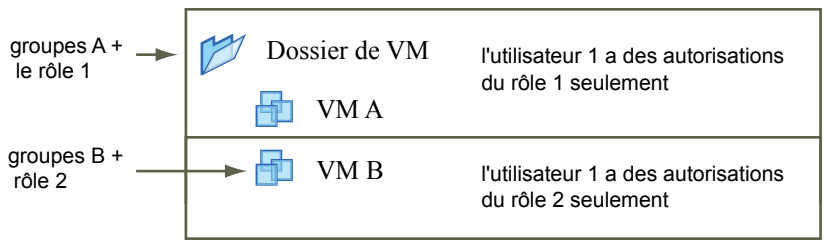
Cet exemple illustre comment les autorisations qui sont assignées sur un objet enfant peuvent ignorer les autorisations qui sont assignées sur un objet parent. Vous pouvez utiliser ce comportement de non prise en compte pour limiter l'accès client à des zones spécifiques de l'inventaire.

Dans cet exemple, des autorisations sont assignées à deux groupes différents sur deux objets 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 4-4. Exemple 2 : Autorisations d'enfant ignorant des autorisations de parent



Exemple 3 : Autorisations d'utilisateurs ignorant des autorisations de groupes

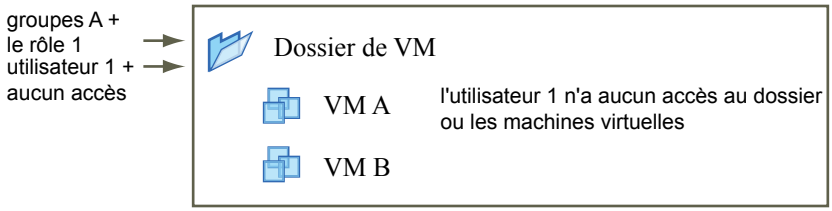
Cet exemple illustre comment des autorisations assignées directement à un utilisateur individuel ignorent les autorisations assignées à un groupe dont l'utilisateur est un membre.

Dans cet exemple, des autorisations sont assignées à un utilisateur et à un groupe sur le même objet.

- 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 ignore l'autorisation de groupes. L'utilisateur 1 n'a aucun accès au dossier ou aux VM A et B. de VM.

Figure 4-5. Exemple 3 : Autorisations d'utilisateurs ignorant des autorisations de groupes



autorisations de l'utilisateur racine

Les utilisateurs racines peuvent uniquement effectuer des actions sur l'hôte auquel ils sont spécifiquement connectés.

Pour des raisons de sécurité, vous ne souhaitez peut-être pas utiliser l'utilisateur racine dans le rôle Administrateur. Dans ce cas, vous pouvez modifier les autorisations après l'installation afin que l'utilisateur racine ne dispose plus des privilèges administratifs ou vous pouvez supprimer entièrement les autorisations d'accès de l'utilisateur racine via vSphere Client. Si vous procédez ainsi, vous devez d'abord créer une autre autorisation au niveau de la racine dont l'utilisateur assigné diffère de celui du rôle Administrateur.

L'assignation du rôle Administrateur à un utilisateur différent vous permet de maintenir la sécurité à travers la traçabilité. vSphere Client enregistre toutes les actions que l'utilisateur du rôle Administrateur initialise comme événements, et vous fournit une piste d'audit. Si tous les administrateurs ouvrent une session en tant qu'utilisateur racine, vous ne pouvez pas savoir quel administrateur a effectué une action. Si vous créez plusieurs autorisations au niveau de la racine (chacune étant associée à un groupe d'utilisateurs ou utilisateur différent) vous pouvez suivre les actions de chaque administrateur ou groupe administratif.

Après avoir créé un autre utilisateur Administrateur, vous pouvez assigner un rôle différent à l'utilisateur racine. Pour gérer l'hôte via vCenter Server, le nouvel utilisateur que vous avez créé doit disposer des privilèges Administrateurs complets sur l'hôte.

Remarque Les commandes `vicfg` n'effectuent pas de contrôle d'accès. Par conséquent, même si vous limitez les privilèges de l'utilisateur racine, cela n'affecte pas ce que l'utilisateur peut faire avec les commandes d'interface de ligne de commande.

---

autorisations de vpxuser

L'autorisation de vpxuser est utilisée par vCenter Server pour gérer les activités de l'hôte. vpxuser est créé lorsqu'un hôte est associé à vCenter Server.

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 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.

autorisations 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 doit être modifié ou utilisé par des utilisateurs interactifs.

Avertissement Ne modifiez en aucun cas l'utilisateur dcui et ne changez pas ses autorisations. Dans le cas contraire, vous risquez d'avoir des difficultés à utiliser l'hôte via l'interface utilisateur local.

Validation d'autorisation

vCenter Server et les hôtes ESXi qui utilisent Active Directory valident régulièrement des utilisateurs et des groupes contre le domaine Windows Active Directory. La validation se produit à chaque fois que le système hôte démarre et à intervalles réguliers spécifiés dans les paramètres de vCenter Server.

Par exemple, si des autorisations étaient assignées à l'utilisateur Smith et que dans le domaine le nom d'utilisateur était changé en Smith2, l'hôte conclut que Smith n'existe plus et supprime les autorisations pour cet utilisateur lors de la validation suivante.

De même, si l'utilisateur Smith est supprimé du domaine, toutes les autorisations sont enlevées quand la prochaine validation se produit. Si un nouvel utilisateur Smith est ajouté au domaine avant que la prochaine validation se produise, le nouvel utilisateur Smith reçoit toutes les autorisations affectées à l'ancien utilisateur Smith.

Assignation d'autorisations

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 assigner les mêmes autorisations en même temps sur des objets multiples en déplaçant les objets vers un dossier et en définissant les autorisations sur le dossier.

Prérequis

Autorisations.Modifier l'autorisation sur l'objet parent de l'objet dont vous voulez modifier les autorisations.

Procédure

1 Sélectionner l'objet et cliquer sur l'onglet **[Autorisations]** .

2 cliquez avec le bouton droit sur l'onglet **[Autorisations]** et sélection **[Ajout d'autorisation]** .

3 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.

4 (Facultatif) Désélectionner la case à cocher **[Propagation aux objets enfant]** .

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

5 Cliquer sur **[Ajout]** pour ouvrir la boîte de dialogue Sélectionner utilisateurs ou groupes.

6 Identifier l'utilisateur ou le groupes à assigner à ce rôle.

   a Sélectionner le domaine où l'utilisateur ou le groupes sont situés depuis le menu déroulant **[Domaine]** .

   b Introduire un nom dans la fenêtre de recherche ou sélection un nom depuis la liste **[Nom]** .

   c Cliquez sur **[Ajouter]** .

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

   d RépétezÉtape 6a les étapes Étape 6c pour ajouter des utilisateurs ou des groupes supplémentaires.

   e Cliquez sur **[OK]** lorsque vous avez terminé.

7 Vérifier que les utilisateurs et les groupes sont affectés aux autorisations appropriées et cliquer sur **[OK]** .

8 Cliquer sur **[OK]** pour terminer.

   Le serveur ajoute l'autorisation à la liste d'autorisations pour l'objet.

   La liste d'autorisations référence tous les utilisateurs et les groupes qui ont des rôles assignés à l'objet et indique où le rôle est assigné dans la hiérarchie de vCenter Server.

Ajuster la liste de recherche dans de grands domaines

Si vous avez des domaines avec des milliers d'utilisateurs ou de groupes ou si les recherches prennent un bon moment pour se terminer, Réglez les paramètres de recherche dans la boîte de dialogue Choisir les utilisateurs ou les groupes.

Remarque Cette procédure s'applique seulement aux listes d'utilisateurs de vCenter Server. Les listes d'utilisateurs d'hôte ESXi ne peuvent pas être recherchées de la même manière.

Prérequis

Pour configurer les paramètres Active Directory, vSphere Client doit être connecté au système vCenter Server.

Procédure

1 Depuis vSphere Client connecté à un système vCenter Server, sélectionnez **[Administration]** > **[Paramètres vCenter Server]** .

2 Dans le volet de navigation, sélectionnez **[Active Directory]** .

3 Modifiez les valeurs si nécessaire.

Option	Description
Délai d'expiration d'Active Directory	Délai d'expiration en secondes pour la connexion au serveur Active Directory. Cette valeur spécifie le laps de temps 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.
Activer la limite de requête	Cochez cette case pour limiter le nombre d'utilisateurs et de groupes qu'affiche vCenter Server dans la boîte de dialogue Ajouter des autorisations pour le domaine sélectionné.
Valeur d'utilisateurs & de groupes	Spécifie le nombre maximum d'utilisateurs et de groupes que vCenter Server affiche depuis le domaine sélectionné dans la boîte de dialogue Sélectionner utilisateurs ou groupes. Si vous entrez 0 (zéro), tous les utilisateurs et groupes apparaissent.

4 Cliquez sur **[OK]** .

Changer les paramètres de validation d'autorisation

vCenter Server valide périodiquement ses listes d'utilisateurs et de groupes contre les utilisateurs et les groupes dans le domaine Windows Active Directory. Il supprime alors les utilisateurs ou les groupes qui n'existent plus dans le domaine. Vous pouvez changer l'intervalle entre les validations.

Procédure

1 Depuis vSphere Client connecté à un système vCenter Server, sélectionnez **[Administration]** > **[Paramètres vCenter Server]** .

2 Dans le volet de navigation, sélectionnez **[Active Directory]** .

3 (Facultatif) Décochez la case **[Activer validation]** pour désactiver la validation.

La validation est activée par défaut. Les utilisateurs et les groupes sont validés quand le système de vCenter Server démarre, même si la validation est désactivée.

4 Si la validation est activée, entrer une valeur dans la case de texte Période de validation pour spécifier le temps, en minutes, s'écoulant entre les validations.

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 Sélectionner un objet dans l'inventaire à partir de vSphere Client.

2 Cliquer sur l'onglet **[Autorisations]** .

3 Cliquer sur l'élément de ligne pour sélectionner l'utilisateur ou le groupes et la paire de rôle.

4 Sélectionnez **[Inventaire]** > **[Autorisations]** > **[Propriétés]** .

5 Sélectionner un rôle pour l'utilisateur ou le groupes du menu déroulant.

6 Pour propager les privilèges aux enfants de l'objet d'inventaire assigné, cliquer sur la case à cocher **[Propager]** et cliquer sur **[OK]** .

Supprimer les autorisations

La suppression d'une autorisation pour un utilisateur ou un groupe ne supprime pas l'utilisateur ou le groupes de la liste de ceux disponibles. Ceci ne supprime pas non plus le rôle de la liste d'éléments disponibles. Ceci supprime l'utilisateur ou le groupe et la paire de rôle de l'objet d'inventaire sélectionné.

Procédure

1 Cliquer sur le bouton **[Inventaire]** du vSphere Client.

2 Développer l'inventaire si nécessaire et cliquer sur l'objet approprié.

3 Cliquer sur l'onglet **[Autorisations]** .

4 Cliquer sur l'élément de ligne approprié pour sélectionner l'utilisateur ou le groupes et la paire de rôle.

5 Sélectionnez **[Inventaire]** > **[Autorisations]** > **[Supprimer]** .

vCenter Server supprime le paramètre d'autorisation.

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 :

- Dans la mesure du possible, accorder les autorisations aux groupes plutôt qu'aux utilisateurs individuels.
- Octroyez des autorisations uniquement lorsque cela est nécessaire.. 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 regrouper les objets afin qu'ils correspondent aux différentes autorisations que vous voulez leur octroyer..
- Soyez prudent lorsque vous accordez une autorisation au niveau racine de vCenter Server. Les utilisateurs ayant des autorisations au niveau racine ont accès à des données globales sur vCenter Server, telles que les rôles, les attributs personnalisés, les paramètres de vCenter Server et les licences. Les modifications apportées aux licences et aux rôles sont appliquées à tous les systèmes vCenter Server dans un groupe Linked Mode, même si l'utilisateur n'a pas l'autorisation d'accéder à tous les systèmes vCenter Server du groupe.
- Dans la plupart des cas, activez la propagation au niveau des autorisations. 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 particulières de la hiérarchie auxquelles vous ne voulez pas que certains utilisateurs aient accès.

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 appropriés d'échantillon.

Le tableau suivant répertorie les tâches courantes qui exigent plusieurs privilèges. Vous pouvez utiliser les rôles applicables sur les objets d'inventaire pour accorder des autorisations pour effectuer ces tâches ou vous pouvez créer vos propres rôles avec les privilèges requis équivalents.

Tableau 4-1. Privilèges requis pour les tâches courantes

Tâche	Privilèges requis	Rôle applicable
Créer une machine virtuelle	Sur le dossier ou le centre de données de destination : ■ **Machine virtuelle.Inventaire.Création brute** ■ **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) ■ **Machine virtuelle.Inventaire.Création brute**	Administrateur de la machine virtuelle
	Sur l'hôte, cluster ou pool de ressources de destination : **Ressource.Attribuer une machine virtuelle au pool de ressources**	Administrateur de la machine virtuelle
	Sur la banque de données ou le dossier de destination contenant une banque de données : **Banque de données.Allouer l'espace**	Utilisateur ou administrateur de la machine virtuelle de la banque de données
	Sur le réseau auquel la machine virtuelle sera assignée : **Mise en réseau.Assigner réseau**	Utilisateur ou administrateur de la machine virtuelle de réseau
Déployer une machine virtuelle à partir d'un modèle	Sur le dossier ou le centre de données de destination : ■ **Machine virtuelle.Inventaire.Création brute** ■ **Machine virtuelle .Configuration.Ajouter un nouveau disque**	Administrateur de la machine virtuelle
	Sur un modèle ou un dossier des modèles : **Machine virtuelle.Provisionnement.Déployer un modèle**	Administrateur de la machine virtuelle
	Sur l'hôte, le cluster ou le pool de ressources de destination : **Ressource.Assigner virtuel.Machine au pool de ressources**	Administrateur de la machine virtuelle
	Sur la banque de données de destination ou le dossier des banques de données : **Banque de données.Allouer l'espace**s	Utilisateur ou administrateur de la machine virtuelle de la banque de données
	Sur le réseau auquel la machine virtuelle sera assignée : **Mise en réseau.Assigner réseau**	Utilisateur ou administrateur de la machine virtuelle de réseau
Faire un snapshot de machine virtuelle	Sur la machine virtuelle ou un dossier des machines virtuelles : **Machine virtuelle.État.Créer un snapshot**s	Utilisateur d'alimentation de machine virtuelle ou administrateur de la machine virtuelle
	Sur la banque de données de destination ou le dossier des banques de données : **Banque de données.Allouer l'espace**	Utilisateur ou administrateur de la machine virtuelle de la banque de données
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 de la machine virtuelle

Tableau 4-1. Privilèges requis pour les tâches courantes (suite)

Tâche	Privilèges requis	Rôle applicable
	Sur le pool de ressources de destination : **Ressource.Attribuer une machine virtuelle au pool de ressources**	Administrateur de la machine virtuelle
Installer un système d'exploitation hôte sur une machine virtuelle	Sur la machine virtuelle ou le dossier des machines virtuelles : ■ **Machine virtuelle.Interaction.Répondre à la question** ■ **Machine virtuelle.Interaction.Interaction de console** ■ **Machine virtuelle.Interaction.Connexion de périphérique** ■ **Machine virtuelle.Interaction.Mettre hors tensions** ■ **Machine virtuelle.Interaction.Mettre sous tension** ■ **Machine virtuelle.Interaction.Réinitialiser** ■ **Machine virtuelle.Interaction.Configurer les supports CD** (si s''installe d'un CD) ■ **Machine virtuelle.Interaction.Configurer le support de disquettes** (si s'installe d'une disquette) ■ **Machine virtuelle.Interaction.Installation d'outils**	Utilisateur d'alimentation de machine virtuelle ou administrateur de la machine virtuelle
	Sur une banque de données contenant l'image ISO de support d'installation : **Banque de données.Parcourir la banque de données** (Si installation à partir d'une image ISO sur une banque de données)	Utilisateur d'alimentation de machine virtuelle ou administrateur de la machine virtuelle
Migrer une machine virtuelle avec vMotion	Sur la machine virtuelle ou le dossier des machines virtuelles : ■ **Ressource.Migrer** ■ **Ressource.Attribuer une machine virtuelle au pool de ressources** (si la destination est un pool de ressources différent de la source)	Administrateur de centre de données ou administrateur de pool de ressources ou administrateur de la machine virtuelle
	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 centre de données ou administrateur de pool de ressources ou administrateur de la machine virtuelle
Migrer à froid (relocaliser) une machine virtuelle	Sur la machine virtuelle ou le dossier des machines virtuelles : ■ **Ressource.Translater** ■ **Ressource.Attribuer une machine virtuelle au pool de ressources** (si la destination est un pool de ressources différent de la source)	Administrateur de centre de données ou administrateur de pool de ressources ou administrateur de la machine virtuelle
	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 centre de données ou administrateur de pool de ressources ou administrateur de la machine virtuelle
	Sur la banque de données de destination (si différent de la source) : **Banque de données.Allouer l'espace**	Utilisateur ou administrateur de la machine virtuelle de la banque de données
Migration d'une machine virtuelle avec Storage vMotion	Sur la machine virtuelle ou le dossier des machines virtuelles : **Ressource.Migrer**	Administrateur de centre de données ou administrateur de pool de ressources ou administrateur de la machine virtuelle

Tableau 4-1. Privilèges requis pour les tâches courantes (suite)

Tâche	Privilèges requis	Rôle applicable
	Sur la banque de données de destination : **Banque de données.Allouer l'espace**	Utilisateur ou administrateur de la machine virtuelle de la banque de données
Déplacer un hôte dans un cluster	Sur l'hôte : **Hôte.Inventaire.Ajouter l'hôte au cluster**	Administrateur ou administrateur de la machine virtuelle de centre de données
	Sur le cluster de destination : **Hôte.Inventaire.Ajouter l'hôte au cluster**	Administrateur ou administrateur de la machine virtuelle de centre de données

Attribution de rôles

vCenter Server et ESXi autorisent l'accès à des objets uniquement aux utilisateurs qui disposent des autorisations appropriées. Lorsque vous assignez des autorisations de groupes ou d'utilisateur pour l'objet, vous devez associer l'utilisateur ou groupes à un rôle. Un rôle est un ensemble prédéfini de privilèges.

Les hôtes ESXi fournissent trois rôles par défaut, et vous ne pouvez pas modifier les privilèges qui leur sont associés. Chaque rôle par défaut suivant inclut les 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 pas des privilèges des rôles par défaut.

Vous pouvez créer des rôles personnalisés en utilisant les fonctionnalités de modification de rôles dans vSphere Client afin de créer des ensembles de privilèges correspondant à vos besoins utilisateurs. Si vous utilisez vSphere Client connecté à vCenter Server afin de gérer vos hôtes ESXi, vous disposez de choix de rôles supplémentaires dans vCenter Server. Par ailleurs, les rôles que vous créez directement sur un hôte ne sont pas accessibles au sein de vCenter Server. Vous pouvez utiliser ces rôles uniquement si vous ouvrez une session de l'hôte directement depuis vSphere Client.

Remarque Si vous ajoutez un rôle personnalisé sans lui attribuer de privilège, il est créé comme rôle Lecture seule avec trois privilèges définis par le système : System.Anonymous, System.View, et System.Read.

Si vous gérez des hôtes ESXi via vCenter Server, la conservation des rôles personnalisés dans l'hôte et vCenter Server peut engendrer la confusion et des utilisations abusives. Dans ce type de configuration, conservez uniquement les rôles personnalisés dans vCenter Server.

Vous pouvez créer des rôles et configurer des autorisations via une connexion directe à l'hôte ESXi.

Utilisation des rôles pour assigner des privilèges

Un rôle est un ensemble prédéfini de privilèges. Les privilèges définissent les droits individuels dont un utilisateur a besoin pour exécuter des actions et pour lire des propriétés.

Quand vous assignez des autorisations à un utilisateur ou à un groupe, vous appariez l'utilisateur ou le groupes avec un rôle et associez cet appariement à un objet d'inventaire. Un simple utilisateur pourrait avoir différents rôles pour différents objets dans l'inventaire. Par exemple, si vous avez deux pools de ressources dans votre inventaire, pool A et pool B, vous pourriez assigner à un utilisateur particulier le rôle d'utilisateur de machine virtuelle sur le pool A et le rôle en lecture seule sur le pool B. Ces affectations permettraient à cet utilisateur d'activer des machines virtuelles dans le pool A, mais pas ceux du pool B. L'utilisateur serait toujours en mesure de consulter l'état des machines virtuelles dans le pool B.

Les rôles créés sur un hôte sont séparés des rôles créés sur un système vCenter Server. Quand vous gérez un hôte à l'aide de vCenter Server, les rôles créés par vCenter Server sont disponibles. Si vous vous connectez directement à l'hôte en utilisant vSphere Client, les rôles créés directement sur l'hôte sont disponibles.

vCenter Server et les hôtes ESXi fournissent des rôles par défaut :

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

Rôles d'échantillon VMware fournit des rôles d'échantillon pour davantage de commodité comme directives et suggestions. Vous pouvez modifier ou supprimer ces rôles.

Vous pouvez également créer des rôles.

Tous les rôles permettent à l'utilisateur de programmer des tâches par défaut. Les utilisateurs peuvent programmer seulement les tâches dont ils ont reçu l'autorisation d'exécution au moment de leur création.

Remarque Les modifications aux autorisations et aux rôles prennent effet immédiatement, même si les utilisateurs impliqués ont ouvert une session. Les recherches sont une exception, les modifications d'autorisation entrant en vigueur après que l'utilisateur se soit déconnecté et reconnecté..

Rôles par défaut pour ESXi et vCenter Server

vCenter Server et ESXi fournissent des rôles par défaut. Ces rôles regroupent des privilèges pour les espaces communs de responsabilité dans un environnement vSphere.

Vous pouvez utiliser les rôles par défaut pour assigner des autorisations dans votre environnement ou les utiliser comme modèle pour développer vos propres rôles.

Tableau 4-2. Rôles par défaut

Rôle	Type de rôle	Description des capacités d'utilisateur
Aucun accès	système	Ne peut pas consulter ou changer l'objet assigné. Les onglets de vSphere Client liés à un objet apparaissent sans contenu. Peut être utilisé pour révoquer les autorisations qui seraient autrement propagées à un objet depuis un objet parent. Disponible dans ESXi et vCenter Server.
Lecture seule	système	Consulter l'état et les détails au sujet de l'objet. Consulter tous les panneaux d'onglet dans vSphere Client excepté l'onglet de console. Ne peut exécuter aucune action par les menus et les barres d'outils. Disponible sur ESXi et vCenter Server.
Administrateur	système	Tous les privilèges pour tous les objets. Ajouter, supprimer et définir des droits d'accès et des privilèges pour tous les utilisateurs de vCenter Server et tous les objets virtuels dans l'environnement de vSphere. Disponible dans ESXi et vCenter Server. **Remarque** Les utilisateurs du groupe Active Directory ESX Admins reçoivent automatiquement le rôle d'Administrateur.
Utilisateur d'alimentation de machine virtuelle	échantillon	Ensemble de privilèges permettant à l'utilisateur d'interagir avec et d'apporter des modifications matérielles aux machines virtuelles, et d'exécuter des opérations de snapshot. Les privilèges accordés incluent : ■ Tous les privilèges pour le groupe de privilèges de tâche planifiée. ■ Les privilèges sélectionnés pour les éléments, la banque de données et les groupes globaux de privilèges de machine virtuelle. ■ Aucun privilège pour les dossiers, le centre de données, le réseau, l'hôte, les ressources, les alarmes, les sessions, les performances et les groupe de privilèges d'autorisations. Habituellement accordé sur un dossier qui contient des machines virtuelles ou sur différentes machines virtuelles. Disponible sur vCenter Server.

Tableau 4-2. Rôles par défaut (suite)

Rôle	Type de rôle	Description des capacités d'utilisateur
Utilisateur de machine virtuelle	échantillon	Ensemble de privilèges permettant à l'utilisateur d'interagir avec une console de machine virtuelle, d'insérer un support et d'effectuer des opérations d'alimentation. N'accorde pas de privilèges pour apporter des modifications matérielles virtuelles à la machine virtuelle. Les privilèges accordés incluent : ■ Tous les privilèges pour le groupe de privilèges de tâche planifiée. ■ Les privilèges sélectionnés pour les éléments et les groupes globaux de privilèges de machine virtuelle. ■ Aucun privilège pour les dossiers, le centre de données, la banque de données, le réseau, l'hôte, les ressources, les alarmes, les sessions, les performances et les groupes de privilèges d'autorisations. Habituellement accordé sur un dossier qui contient des machines virtuelles ou sur différentes machines virtuelles. Disponible sur vCenter Server.
Administrateur de pool de ressources	échantillon	Ensemble de privilèges permettant à l'utilisateur de créer des pools de ressources enfant et de modifier la configuration des enfants, mais pas de modifier la configuration du pool ou du cluster sur lequel le rôle a été assigné. Permet également à l'utilisateur d'accorder des autorisations aux pools de ressources enfant et assigne des machines virtuelles aux pools de parent ou de ressources enfant. Les privilèges accordés incluent : ■ Tous les privilèges pour le dossier, la machine virtuelle, les alarmes et les groupe de privilèges de tâche planifiée. ■ Les privilèges sélectionnés pour des groupes de privilèges de ressource et d'autorisations. ■ Aucun privilège pour les dossiers, le centre de données, le réseau, l'hôte, les ressources, les alarmes, les sessions, les performances et les groupe de privilèges d'autorisations. Des privilèges supplémentaires doivent être octroyés sur les machines virtuelles et les banques de données pour permettre le provisionnement de nouvelles machines virtuelles. Habituellement accordé sur un cluster ou un pool de ressources. Disponible sur vCenter Server.
Utilisateur de banque de données	échantillon	Ensemble de privilèges permettant à l'utilisateur d'utiliser de l'espace sur les banques de données sur lesquelles ce rôle est octroyé. Pour exécuter une opération d'utilisation d'espace, telle que créer un disque virtuel ou faire un snapshot, l'utilisateur doit également avoir les privilèges appropriés de machine virtuelle accordés pour ces opérations. Habituellement accordé sur une banque de données ou un dossier de banques de données. Ce rôle est disponible sur vCenter Server.
Utilisateur de réseau	échantillon	Ensemble de privilèges permettant à l'utilisateur d'affecter des machines virtuelles ou des hôtes aux réseaux, si les autorisations appropriées pour l'affectation sont également octroyées sur les machines virtuelles ou les hôtes. Habituellement accordé sur un réseau ou un dossier de réseaux. Disponible sur vCenter Server.

Créer un rôle

VMware recommande de créer des rôles 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 d'un groupe connecté dans vCenter Linked Mode, les modifications effectuées sont propagées à tous les autres systèmes vCenter Server du groupes. Cependant, les affectations des rôles à des utilisateurs et objets spécifiques ne sont pas partagées parmi les systèmes vCenter Server liés.

Prérequis

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

Procédure

1 Dans la page d'accueil de vSphere Client, cliquer sur **[Rôles]** .

2 Faire un clic droit sur le panneau d'informations de l'onglet **[Rôles]** et cliquer sur **[Ajout]** .

3 Introduire un nom pour le nouveau rôle.

4 Sélectionner les privilèges pour le rôle et cliquer sur **[OK]** .

Cloner un rôle

Vous pouvez faire une copie d'un rôle existant, le renommer et l'éditer plus tard. 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 d'un groupe connecté dans le vCenter Linked Mode, les modifications effectuées sont propagées à tous les autres systèmes vCenter Server du groupes. Cependant, les affectations des rôles à des utilisateurs et objets spécifiques ne sont pas partagées parmi les systèmes vCenter Server liés.

Prérequis

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

Procédure

1 Dans la page d'accueil de vSphere Client, cliquer sur **[Rôles]** .

2 Pour sélectionner le rôle à reproduire, cliquer sur l'objet dans la liste **[Rôles]** .

3 Pour cloner le rôle sélectionné, sélectionnez **[Administration]** > **[Rôle]** > **[Cloner]** .

Un doublon du rôle est ajouté à la liste de rôles. Le nom est `Copie de`*`Nom de rôle`*.

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 groupes assigné au rôle édité.

Si vous créez ou modifiez un rôle sur un système vCenter Server qui fait partie d'un groupe connecté dans vCenter Linked Mode, les modifications effectuées sont propagées à tous les autres systèmes vCenter Server du groupes. Cependant, les attributions de rôles à des utilisateurs et objets spécifiques ne sont pas partagées dans les systèmes vCenter Server liés.

Prérequis

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

Procédure

1 Dans la page d'accueil de vSphere Client, cliquer sur **[Rôles]** .

2 Cliquez avec le bouton droit sur le rôle à modifier et sélectionnez **[Modifier rôle]** .

3 Sélectionner les privilèges pour le rôle et cliquer sur **[OK]** .

Supprimer un rôle

Quand vous supprimez un rôle qui n'est assigné à aucun utilisateur ou groupes, la définition est supprimée de la liste de rôles. Quand vous supprimez un rôle qui est assigné à un utilisateur ou à un groupe, vous pouvez supprimer des affectations ou les remplacer par une affectation à un autre rôle.

Avertissement Vous devez comprendre comment les utilisateurs seront affectés avant de supprimer toutes les affectations ou de les substituer. Les utilisateurs qui n'ont aucune autorisation accordée ne peuvent pas ouvrir une session sur vCenter Server.

Prérequis

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

Si vous supprimez un rôle d'un système de vCenter Server qui fait partie d'un groupe connecté en Linked Mode, contrôlez l'utilisation de ce rôle sur les autres systèmes de vCenter Server au sein du groupe. La suppression d'un rôle d'un système de vCenter Server supprime le rôle de tous les autres systèmes de vCenter Server au groupes, même si vous attribuez à nouveau des autorisations à un autre rôle sur le système actuel de vCenter Server.

Procédure

1 Dans la page d'accueil de vSphere Client, cliquer sur **[Rôles]** .

2 Cliquer sur l'objet que vous voulez supprimer dans la liste de rôles.

3 Sélectionnez **[Administration]** > **[Rôle]** > **[Supprimer]** .

4 Cliquez sur **[OK]** .

   Le rôle est supprimé de la liste.

   Si le rôle est assigné à un utilisateur ou à un groupe, un message d'avertissement apparaît.

5 Sélectionnez une option de réaffectation et cliquez sur **[OK]** .

Option	Description
Supprimer les affectations de rôle	Supprime un utilisateur ou un groupe configuré et le rôle d'appariement sur le serveur. Si un utilisateur ou un groupe ne disposent pas d'autres autorisations affectées, ils perdent tous les privilèges.
Réassigner des utilisateurs affectés à	Attribue à nouveau n'importe quel utilisateur ou groupes et rôle configurés d'appariement au nouveau rôle sélectionné.

Renommer un rôle

Quand vous renommez un rôle, aucune modification ne se produit au niveau des affectations de ce rôle.

Si vous créez ou modifiez un rôle sur un système vCenter Server qui fait partie d'un groupe connecté dans Linked Mode, les modifications effectuées sont propagées aux autres systèmes vCenter Server du groupe. Cependant, les affectations des rôles à des utilisateurs et objets spécifiques ne sont pas partagées parmi les systèmes vCenter Server liés.

Prérequis

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

Procédure

1 Dans la page d'accueil de vSphere Client, cliquer sur **[Rôles]** .

2 Cliquer sur l'objet dans la liste de rôles que vous voulez renommer.

3 Sélectionnez **[Administration]** > **[Rôle]** > **[Renommez]** .

4 Saisir le nouveau nom.

Accès à l'interface utilisateur de console directe (DCUI)

Seuls les utilisateurs assignés au rôle Administrateur peuvent se connecter à l'interface utilisateur de console directe (DCUI). Pour autoriser l'accès à la console directe, ajoutez l'utilisateur au groupe d'administrateurs locaux.

Procédure

1 Connectez-vous à ESXi en utilisant vSphere Client.

2 Cliquez sur l'onglet **[Utilisateurs et groupes locaux]** et sur **[Utilisateurs]** .

3 Cliquez avec le bouton droit sur l'utilisateur, puis cliquez sur **[Modifier]** pour ouvrir la boîte de dialogue Modifier l'utilisateur.

4 À partir du menu déroulant **[groupes]** , sélectionnez localadmin et cliquez sur **[Ajouter]** .

5 Cliquez sur **[OK]** .

Utiliser Active Directory pour gérer les utilisateurs et les groupes

Vous pouvez configurer l'hôte ESXi pour utiliser un service d'annuaire, tel que Active Directory, pour gérer les utilisateurs et les groupes d'utilisateurs.

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

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 pleinement qualifié par 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.

   ESXi prend en charge la synchronisation du temps à l'aide d'un serveur externe NTPv3 ou NTPv4 qui est conforme à RFC 5905 et RFC 1305. Le service Microsoft Windows W32Time ne remplit pas ces conditions.

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

   a Dans vSphere Client, sélectionnez l'hôte dans l'inventaire.

   b Cliquez sur l'onglet **[Configuration]** puis sur **[DNS et routage]** .

c Cliquez sur le lien **[Propriétés]** en haut à droite du panneau.

d Dans la boîte de dialogue Configuration de routage, vérifiez que le nom de l'hôte et les informations sur le serveur DNS de l'hôte sont correctes.

Suivant

Utilisez vSphere Client pour rejoindre un domaine de service d'annuaire.

Ajouter un hôte à un domaine de service d'annuaire

Pour utiliser un service d'annuaire, vous devez joindre l'hôte au domaine de 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 (service CAM), voir « Utiliser vSphere Authentication Proxy pour ajouter un hôte à un domaine », page 75.

Prérequis

Vérifiez que vSphere Client est connecté à un système vCenter Server ou à l'hôte.

Procédure

1 Sélectionnez un hôte dans l'inventaire du vSphere Client et cliquez sur l'onglet **[Configuration]** .

2 Cliquez sur **[Propriétés]** .

3 Dans la boîte de dialogue Configuration des services d'annuaire, sélectionnez le service d'annuaire dans le menu déroulant.

4 Entrez un domaine.

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

5 Cliquez sur **[Joindre le domaine]** .

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 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 Sélectionnez un hôte dans l'inventaire du vSphere Client et cliquez sur l'onglet **[Configuration]** .

2 Sous Logiciel, sélectionnez **[Services d'authentification]** .

   La page Paramètre des services d'authentification affiche les paramètres du service d'annuaire et du domaine.

Utiliser vSphere Authentication Proxy

Lorsque vous utilisez vSphere Authentication Proxy, il est inutile de transmettre les données d'identification Active Directory à l'hôte. Les utilisateurs entrent le nom de domaine du serveur Active Directory et l'adresse IP du serveur proxy d'authentification lorsqu'ils ajoutent un hôte à un domaine.

Installer le service vSphere Authentication Proxy

Pour utiliser le service vSphere Authentication Proxy (service CAM) pour l'authentification, vous devez installer le service sur une machine hôte.

Vous pouvez installer vSphere Authentication Proxy sur la même machine que le système vCenter Server associé ou sur une machine différente disposant d'une connexion réseau au vCenter Server. vSphere Authentication Proxy n'est pas compatible avec les versions vCenter Server antérieures à la version 5.0.

Le service vSphere Authentication Proxy se lie à une adresse IPv4 pour communiquer avec vCenter Server, et ne prend pas en charge IPv6. vCenter Server peut être installé sur une machine hôte exclusivement en mode IPv4, en mode mixte IPv4/IPv6 ou exclusivement en mode IPv6, mais la machine qui se connecte à vCenter Server via vSphere Client doit disposer d'une adresse IPv4 pour que le service vSphere Authentication Proxy fonctionne.

Prérequis

- Vérifiez que vous disposez des privilèges d'administrateur sur la machine hôte sur laquelle vous installez le service vSphere Authentication Proxy.
- Vérifiez que la machine hôte utilise Windows Installer 3.0 ou une version ultérieure.
- Vérifiez que la machine hôte est dotée d'un processeur et d'un système d'exploitation compatibles. vSphere Authentication Proxy prend en charge les mêmes processeurs et systèmes d'exploitation que vCenter Server.
- Vérifiez que la machine hôte possède une adresse IPv4 valide. Vous pouvez installer vSphere Authentication Proxy sur une machine hôte exclusivement en mode IPv4 ou en mode mixte IPv4/IPv6, mais vous ne pouvez pas installer vSphere Authentication Proxy sur une machine hôte en mode IPv6.
- Si vous installez vSphere Authentication Proxy sur une machine hôte Windows Server 2008 R2, téléchargez et installez le correctif logiciel Windows décrit dans Windows KB Article 981506 sur le site Web support.microsoft.com. Si vous n'installez pas ce correctif, l'initialisation d'Authentication Proxy Adapter échoue. Ce problème est accompagné de messages d'erreur consignés dans `camadapter.log` similaires à `Échec de la liaison du site Web CAM avec CTL` et `Échec de l'initialisation de CAMAdapter.`

Collectez les informations suivantes pour terminer l'installation :

- L'emplacement d'installation de vSphere Authentication Proxy si vous n'utilisez pas l'emplacement par défaut.
- L'adresse IP ou le nom d'hôte, le port HTTP et les informations d'identification du système vCenter Server auquel vSphere Authentication Proxy doit se connecter.
- Le nom d'hôte ou l'adresse IP pour identifier la machine hôte vSphere Authentication Proxy sur le réseau.

Procédure

1. Sur la machine hôte sur laquelle vous avez installez le service vSphere Authentication Proxy, installez .NET Framework 3.5.
2. Installez vSphere Auto Deploy.

   Il n'est pas nécessaire d'installer Auto Deploy sur la même machine hôte que le service vSphere Authentication Proxy.

3 Ajoutez au domaine la machine hôte sur laquelle vous aller installer le service proxy d'authentification.

4 Utilisez le compte Administrateur de domaine pour vous connecter à la machine hôte.

5 Dans l'inventaire du logiciel d'installation, faites un double clic sur le fichier `autorun.exe` pour lancer l'installation.

6 Sélectionnez **[VMware vSphere Authentication Proxy]** et cliquez sur **[Installer]** .

7 Suivez les invites de l'assistant pour terminer l'installation.

   Au cours de l'installation, le service d'authentification s'enregistre dans l'instance vCenter Server où Auto Deploy est enregistré.

Le service de proxy d'authentification est installé sur la machine hôte.

Remarque Lorsque vous installez le service vSphere Authentication Proxy, le programme d'installation crée un compte de domaine avec les privilèges appropriés pour exécuter le service proxy d'authentification. Le nom de compte commence par le préfixe `CAM-` et possède un mot de passe de 32 caractères généré de manière aléatoire . Le mot de passe n'expire jamais. Ne changez pas les paramètres du compte.

Suivant

Configurez l'hôte pour utiliser le service de proxy d'authentification pour rejoindre le domaine.

Configurer un hôte pour utiliser vSphere Authentication Proxy pour l'authentification

Après avoir installé le service vSphere Authentication Proxy (service CAM), vous devez configurer l'hôte pour utiliser le serveur proxy d'authentification pour authentifier les utilisateurs.

Prérequis

Installez le service vSphere Authentication Proxy (service CAM) sur un hôte, comme décrit dans « Installer le service vSphere Authentication Proxy », page 71.

Procédure

1 Utilisez IIS manager sur l'hôte pour définir la plage DHCP.

   Définir la plage permet aux hôtes utilisant le DHCP dans le réseau de gestion d'utiliser le service de proxy d'authentification.

Option	Action
Pour IIS 6	a Naviguez jusqu'au **[Site Web de gestion des comptes d'ordinateur]** . b Cliquez avec le bouton droit sur le répertoire virtuel **[CAM ISAPI]** . c Sélectionnez **[Propriétés]** > **[Sécurité du répertoire]** > **[Modifier l'adresse IP et les restrictions de nom de domaine]** > **[Ajouter un groupe d'ordinateurs]** .
Pour IIS 7	a Naviguez jusqu'au **[Site Web de gestion des comptes d'ordinateur]** . b Cliquez sur le répertoire virtuel **[CAM ISAPI]** du volet gauche et ouvrez **[Adresse IPv4 et restrictions de domaine]** . c Sélectionnez **[Ajouter entrée autorisée]** > **[Plage d'adresse IPv4]** .

2 Si un hôte n'est pas provisionné par Auto Deploy, remplacez le certificat SSL par défaut par un certificat auto-signé ou par un certificat signé par une autorité de certification (CA) privée.

Option	Description
Certificat auto-signé	Si vous remplacez le certificat par défaut par un certificat auto-signé, ajoutez l'hôte à vCenter Server afin que le serveur proxy d'authentification fasse confiance à l'hôte.
Certificat signé par la CA	Ajoutez le certificat signé par la CA (format Windows uniquement) au magasin des certificats de confiance du système où est installé le service proxy d'authentification et redémarrez le service vSphere Authentication Proxy Adapter. ■ Pour Windows 2003, copiez le fichier du certificat sur `C:\Documents and Settings\All Users\Application Data\VMware\vSphere Authentication Proxy\trust`. ■ Pour Windows 2008, copiez le fichier du certificat sur `C:\Program Data\VMware\vSphere Authentication Proxy\trust`.

Authentification de vSphere Authentication Proxy sur ESXi

Avant d'utiliser vSphere Authentication Proxy pour connecter l'ESXi à un domaine, vous devez authentifier le serveur vSphere Authentication Proxy sur ESXi. Si vous utilisez des profils d'hôte pour vous connecter à un domaine avec le serveur vSphere Authentication Proxy, vous n'avez pas à authentifier le serveur. Le profil d'hôte authentifie le serveur proxy sur ESXi.

Pour authentifier l'ESXi afin d'utiliser vSphere Authentication Proxy, exportez le certificat du serveur du système vSphere Authentication Proxy et importez-le dans ESXi. Vous ne devez authentifier le serveur qu'une seule fois.

Remarque Par défaut, l'ESXidoit authentifier le serveur vSphere Authentication Proxy lorsqu'il l'utilise pour rejoindre un domaine. Assurez-vous que cette fonction d'authentification est toujours activée. Si vous désactivez l'authentification, vous pouvez utiliser la boîte de dialogue Paramètres avancés pour définir l'attribut `UserVars.ActiveDirectoryVerifyCAMCertifcate` sur 0.

Exporter le certificat de vSphere Authentication Proxy

Pour authentifier vSphere Authentication Proxy dans ESXi, vous devez fournir à ESXi le certificat du serveur proxy.

Prérequis

Installez le service vSphere Authentication Proxy (service CAM) sur un hôte, comme décrit dans « Installer le service vSphere Authentication Proxy », page 71.

Procédure

1 Sur le système du serveur proxy d'authentification, utilisez IIS Manager pour exporter le certificat.

Option	Action
Pour IIS 6	a Cliquez avec le bouton droit de la souris sur **[Site Web de gestion des comptes d'ordinateur]** . b Sélectionnez **[Propriétés]** > **[Sécurité d'annuaire]** > **[Afficher le certificat]** .
Pour IIS 7	a Cliquez sur **[Site Web de gestion des comptes d'ordinateur]** dans le volet de gauche. b Sélectionnez **[Liaisons]** pour ouvrir la boîte de dialogue Liaisons de sites. c Sélectionnez la liaison **[https]** . d Select **[Éditer]** > **[Afficher le certificat SSL]** .

2 Sélectionnez **[Détails]** > **[Copier vers un fichier]** .

3 Sélectionnez les options **[Ne pas exporter la clé privée]** et **[X.509 codé en base 64 (CER)]** .

Suivant

Importez le certificat vers ESXi.

Importer un certificat de serveur vSphere Authentication Proxy Server vers ESXi

Pour authentifier le serveur vSphere Authentication Proxy Server dans ESXi, téléchargez le certificat du serveur proxy à ESXi.

Vous utilisez l'interface utilisateur vSphere Client pour télécharger le certificat du serveur vSphere Authentication Proxy à ESXi.

Prérequis

Installez le service vSphere Authentication Proxy (service CAM) sur un hôte, comme décrit dans « Installer le service vSphere Authentication Proxy », page 71.

Exportez le certificat du serveur vSphere Authentication Proxy comme décrit dans « Exporter le certificat de vSphere Authentication Proxy », page 73.

Procédure

1 Sélectionnez un hôte dans l'inventaire vSphere Client et cliquez sur l'onglet **[Résumé]** .

2 Téléchargez le certificat du serveur proxy d'autentification vers un emplacement temporaire sur ESXi.

   a Sous Ressources, cliquez avec le bouton droit sur la banque de données et sélectionnez **[Parcourir la banque de données]** .

   b Sélectionnez l'emplacement du certificat et sélectionnez le bouton **[Télécharger le fichier]** .

   c Accédez au certificat et sélectionnez **[Ouvrir]** .

3 Sélectionnez l'onglet **[Configuration]** et cliquez sur **[Services d'authentification]** .

4 Cliquez sur **[Importer un certificat]** .

5 Entrez le chemin complet du certifcat du serveur proxy d'authentification sur l'hôte et l'adresse IP du serveur proxy d'authentifciation.

   Utilisez le format [*datastore name*] *file path* pour entrer le chemin d'accès au serveur proxy.

6 Cliquez sur **[Importer]** .

Suivant

Configurez l'hôte pour utiliser le serveur vSphere Authentication Proxy afin d'authentifier les utilisateurs.

Utiliser vSphere Authentication Proxy pour ajouter un hôte à un domaine

Lorsque vous joignez un hôte à un domaine de service d'annuaire, vous pouvez utiliser le serveur vSphere Authentication Proxy pour l'authentification au lieu de transmettre les informations d'identification Active Directory fournies par l'utilisateur.

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

- Vérifiez que vSphere Client est connecté à un système vCenter Server ou à l'hôte.
- Si ESXi est configuré avec une adresse DHCP, configurez une plage DHCP comme décrit dans « Configurer un hôte pour utiliser vSphere Authentication Proxy pour l'authentification », page 72.
- Si ESXi est configuré avec une adresse IP statique, vérifiez que son profil associé est configuré pour utiliser le service vSphere Authentication Proxy pour rejoindre un domaine afin que le serveur proxy d'authentification puisse faire confiance à l'adresse IP ESXi.
- Si ESXi utilise un certificat autosigné, vérifiez que l'hôte a été ajouté à vCenter Server. Ainsi, le serveur proxy d'authentification peut faire confiance à ESXi.
- Si ESXi utilise un certificat signé par une autorité de certification et qu'il n'est pas provisionné par Auto Deploy, vérifiez que le certificat de l'autorité de certification a été ajouté au magasin local des certificats de confiance du serveur proxy d'authentification, comme décrit dans « Configurer un hôte pour utiliser vSphere Authentication Proxy pour l'authentification », page 72.
- Authentifiez le serveur vSphere Authentication Proxy sur l'hôte comme décrit dans « Authentification de vSphere Authentication Proxy sur ESXi », page 73.

Procédure

1. Dans l'inventaire de vSphere Client, sélectionnez l'hôte.
2. Sélectionnez l'onglet **[Configuration]** et cliquez sur **[Services d'authentification]** .
3. Cliquez sur **[Propriétés]** .
4. Dans la boîte de dialogue Configuration des services d'annuaire, sélectionnez le service d'annuaire dans le menu déroulant.
5. Entrez un domaine.

   Utilisez le format **`name.tld`** ou **`name.tld/container/path`**.
6. Cochez la case **[Utiliser vSphere Authentication Proxy]** .
7. Entrez l'adresse IP du serveur proxy d'authentification.
8. Cliquez sur **[Joindre le domaine]** .
9. Cliquez sur **[OK]** .

Afficher les paramètres de vSphere Authentication Proxy

Vous pouvez vérifier l'adresse IP et le port où le serveur proxy écoute.

Après avoir installé un service vSphere Authentication Proxy sur une machine hôte, vous pouvez afficher les informations d'adresse de machine hôte et de port dans vSphere Client.

Procédure

- Dans vSphere Client, sélectionnez **[Inventaire] > [Administration] > [vSphere Authentication Proxy]** .

  La page VMware vSphere Authentication Proxy s'ouvre.

Chiffrement et certificats de sécurité pour ESXi et vCenter Server

5

ESXi et vCenter Server utilisent des certificats X.509 version 3 (X.509v3) standard pour chiffrer les informations de session envoyées sur les connexions SSL entre les composants. Si SSL est activé, les données sont privées, protégées, et ne peuvent pas être modifiées en transit sans détection.

Tout le trafic réseau est chiffré tant que les conditions suivantes sont vraies :

- Vous n'avez pas modifié le service proxy Web afin d'autoriser un trafic non chiffré pour le port.
- Votre pare-feu est configuré sur sécurité moyenne ou élevée.

Le contrôle de certificat est activé par défaut et les certificats SSL sont utilisés pour chiffrer le trafic réseau. Néanmoins, ESXi et vCenter Server utilisent des certificats générés automatiquement, créés lors du processus d'installation et stockés sur le système du serveur. Ces certificats sont uniques et permettent de commencer à utiliser le serveur, mais ils ne sont pas vérifiables et ne sont pas signés par une autorité de certification de confiance (CA). Ces certificats par défaut sont vulnérables aux éventuelles attaques de l'intercepteur.

Pour bénéficier de tous les avantages du contrôle des certificats, notamment si vous tentez d'utiliser des connexions à distance chiffrées en externe, installez les nouveaux certificats signés par une autorité de certification interne valide ou achetez un certificat auprès d'une autorité de sécurité de confiance. Le remplacement des certificats vCenter Server est décrit dans la documentation *Exemples et scénarios vSphere*

Remarque Si le certificat auto-signé est utilisé, les clients reçoivent un avertissement pour ce certificat. Pour résoudre ce problème, installez un certificat signé par une autorité de certification reconnue. Si des certificats signés par une CA ne sont pas installés, toute communication entre vCenter Server et les clients vSphere est chiffrée via un certificat auto-signé. Ces certificats ne fournissent pas la sécurité d'authentification requise dans un environnement de production.

Le certificat est composé de deux fichiers : le certificat lui-même (`rui.crt`) et le fichier de clé privée (`rui.key`).

Tableau 5-1. Emplacement par défaut des fichiers de certificat d'ESXi et de vCenter Server

Serveur	Emplacement
ESXi 5.0	`/etc/vmware/ssl/`
vCenter Server (Windows 2008)	`C:\Program Data\VMware\VMware VirtualCenter\SSL`
vCenter Server (Windows 2003)	`C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\SSL`

Ce chapitre aborde les rubriques suivantes :

Activer le contrôle de certificats et vérifier les empreintes hôtes

Pour empêcher les attaques de l'intercepteur et bénéficier entièrement de la sécurité fournie par les certificats, le contrôle de certificats est activé par défaut. Vous pouvez vérifier que le contrôle de certificats est activé dans vSphere Client.

Remarque Les certificats vCenter Server sont conservés à travers les mises à niveau.

Procédure

1 Ouvrez une session sur le système vCenter Server en utilisant vSphere Client.

2 Sélectionnez **[Administration]** > **[Paramètres vCenter Server]** .

3 Cliquez sur **[Paramètres SSL]** dans le volet gauche et vérifiez que **[Vérifier les certificats de l'hôte]** est sélectionné.

4 Si les hôtes requièrent une validation manuelle, comparez les empreintes listées pour les hôtes aux empreintes dans la console de l'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.

5 Si l'empreinte correspond, cochez la case **[Vérifier]** à côté de l'hôte.

   Les hôtes non sélectionnés sont déconnectés après avoir cliqué sur **[OK]** .

6 Cliquez sur **[OK]** .

Générer de nouveaux certificats pour ESXi

En règle générale, vous générez de nouveaux certificats uniquement si vous changez le nom de l'hôte ou supprimez accidentellement le certificat. Dans certaines circonstances, vous devrez peut-être forcer l'hôte à générer de nouveaux certificats.

Procédure

1 Connectez-vous au Shell ESXi et obtenez les privilèges root. **[]**

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

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

   Remarque Si vous régénérez des certificats parce que vous les avez supprimés, cette étape est inutile.

3 Exécutez la commande `/sbin/generate-certificates` pour générer de nouveaux certificats.

4 Exécutez la commande `/etc/init.d/hostd restart` pour redémarrer le processus `hostd`.

5 Vérifiez que l'hôte a généré les nouveaux certificats en utilisant la commande suivante et en comparant les horodatages des nouveaux fichiers de certificat à `orig.rui.crt` et `orig.rui.key`.

```
ls -la
```

Remplacer un certificat d'hôte par défaut par un certificat signé par une autorité de certification

L'hôte ESXi utilise des certificats générés automatiquement, créés lors du processus d'installation. Ces certificats sont uniques et permettent de commencer à utiliser le serveur, mais ils ne sont pas vérifiables et ne sont pas signés par une autorité de certification approuvée (CA).

L'utilisation de certificats par défaut n'est peut-être pas conforme aux règles de sécurité de votre organisation. Si vous avez besoin d'un certificat d'une autorité de certification approuvée, vous pouvez remplacer le certificat par défaut.

Remarque Si l'option Vérifier les certificats est activée dans l'hôte, le remplacement du certificat par défaut peut provoquer l'arrêt de la gestion de l'hôte par vCenter Server. Si le nouveau certificat n'est pas vérifiable par vCenter Server, vous devez reconnecter l'hôte à l'aide du vSphere Client.

ESXi prend en charge uniquement les certificats X.509 pour chiffrer les informations de session envoyées sur les connexions SSL entre les composants du serveur et du client.

Remarque Pour plus d'informations sur le remplacement des certificats par défaut sur un système vCenter Server, consultez la documentation *Exemples et scénarios vSphere*.

Prérequis

Tous les transferts de fichiers et autres communications se produisent lors d'une session HTTPS sécurisée. L'utilisateur servant à authentifier la session doit posséder le privilège **Hôte.Config.AdvancedConfig** sur l'hôte. Pour plus d'informations sur les privilèges ESXi, reportez-vous à la section Chapitre 4, « Authentification et gestion d'utilisateurs », page 45.

Procédure

1 Connectez-vous au Shell ESXi et obtenez les privilèges racine.

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 le nouveau certificat et la clé dans `/etc/vmware/ssl`.

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

5 Redémarrez le processus `hostd` :

```
/etc/init.d/hostd restart
```

Télécharger un certificat SSL et une clé à l'aide d'un HTTPS PUT

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

Procédure

1 Dans votre application de chargement, ouvrez le fichier.

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

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

3 Dans l'interface utilisateur de console directe (DCUI), utilisez l'opération Redémarrer les agents de gestion pour initialiser les paramètres.

Charger une clé SSH à l'aide d'un 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.

Remarque Le mode de verrouillage ne s'applique pas aux utilisateurs racine qui se connectent en utilisant des clés autorisées. Lorsque vous utilisez un fichier de clés autorisées pour authentifier les utilisateurs racine, ces derniers ne sont pas empêchés d'accéder à un hôte avec SSH lorsque l'hôte est verrouillé.

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 à l'un de ces emplacements.

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 des privilèges de l'utilisateur racine pour télécharger ce fichier.
Clés DSA	`https://`*`hostname or IP address`*`/host/ssh_host_dsa_key`
Clés DSA publiques	`https://`*`hostname or ip`*`/host/ssh_host_dsa_key_pub`
Clés RSA	`https://`*`hostname or ip`*`/host/ssh_host_rsa_key`
Clés RSA publiques	`https://`*`hostname or ip`*`/host/ssh_host_rsa_key_pub`

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

Vous pouvez utiliser des clés autorisées pour ouvrir une session sur un hôte avec SSH. Vous pouvez charger les clés autorisées à l'aide d'une commande `vifs`.

Remarque Le mode de verrouillage ne s'applique pas aux utilisateurs racine qui se connectent en utilisant des clés autorisées. Lorsque vous utilisez un fichier de clés autorisées pour authentifier les utilisateurs racine, ces derniers ne sont pas empêchés d'accéder à un hôte avec SSH lorsque l'hôte est verrouillé.

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 DSA
- Clé DSA publique
- Clé RSA
- Clé RSA publique

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

Procédure

◆ Dans l'invite de commande, utilisez la commande `vifs` pour charger la clé SSH à l'emplacement approprié.

```
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 disposer des privilèges de l'utilisateur racine pour télécharger ce fichier.
Clés DSA	`/host/ssh_host_dsa_key`
Clés DSA publiques	`/host/ssh_host_dsa_key_pub`
Clés RSA	`/host/ssh_host_rsa_key`
Clés RSA publiques	`/host/ssh_host_rsa_key_pub`

Configurer les délais d'attente SSL

Vous pouvez configurer les délais d'attente SSL pour ESXi.

Des périodes d'attente peuvent être définies pour deux types de connexions inactives :

- Le paramètre Délai d'attente de lecture s'applique aux connexions qui ont complété le processus de négociation SSL avec le port 443 d'ESXi.
- Le paramètre Délai d'expiration de négociation s'applique aux connexions qui n'ont pas complété le processus de négociation SSL avec le port 443 d'ESXi.

Les délais d'attente des deux connexions sont en millisecondes.

Les connexions inactives sont déconnectées après la période d'attente. Par défaut, les connexions SSL totalement établies ont un délai d'attente d'infini.

Procédure

1 Connectez-vous au Shell ESXi et obtenez les privilèges racine.

2 Passez au répertoire `/etc/vmware/hostd/`.

3 Utilisez un éditeur de texte pour ouvrir le fichier `config.xml`.

4 Saisissez la valeur `<readTimeoutMs>` en millisecondes.

   Par exemple, pour régler le délai d'attente de lecture à 20 secondes, saisissez la commande suivante :

   ```
   <readTimeoutMs>20000</readTimeoutMs>
   ```

5 Saisissez la valeur `<handshakeTimeoutMs>` en millisecondes.

   Par exemple, pour régler le délai d'expiration de négociation à 20 secondes, saisissez la commande suivante :

   ```
   <handshakeTimeoutMs>20000</handshakeTimeoutMs>
   ```

6 Enregistrez les modifications et fermez le fichier.

7 Redémarrez le processus `hostd` :

   ```
   /etc/init.d/hostd restart
   ```

Exemple : Fichier de configuration

La section suivante du fichier `/etc/vmware/hostd/config.xml` indique où entrer les paramètres de délai d'attente SSL.

```
<vmacore>
 ...
 <http>
  <readTimeoutMs>20000</readTimeoutMs>
 </http>
 ...
 <ssl>
  ...
  <handshakeTimeoutMs>20000</handshakeTimeoutMs>
  ...
    </ssl>
</vmacore>
```

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 pas de certificats à l'aide d'expressions relatives au mot de passe. ESXi ne prend pas en charge les expressions relatives au mot de passe, aussi connues comme clés chiffrées. Si vous configurez une expression relative au mot de passe, les processus ESXi ne peuvent pas correctement démarrer.

- Vous pouvez configurer le proxy Web afin qu'il recherche des certificats dans un emplacement autre que celui par défaut. Cette fonctionnalité s'avère utile pour les entreprises qui préfèrent centraliser leurs certificats sur une seule machine afin que plusieurs hôtes puissent les utiliser.

Avertissement Si des certificats ne sont pas stockés localement sur l'hôte (s'ils sont, par exemple, stockés sur un partage NFS), l'hôte ne peut pas accéder à ces certificats si ESXi perd la connectivité réseau. Par conséquent, un client se connectant à l'hôte ne peut pas participer à un protocole de transfert SSL sécurisé avec l'hôte.

- Pour prendre en charge le chiffrement de noms d'utilisateur, de mot de passe et de paquets, SSL est activé par défaut pour les connexions de 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 vCenter Server à niveau, le certificat est conservé.

Configurer le Proxy Web pour rechercher des certificats dans des emplacements non définis par défaut

Vous pouvez configurer le proxy Web afin qu'il recherche des certificats dans un emplacement autre que celui par défaut. Ceci s'avère utile pour les entreprises qui préfèrent centraliser leurs certificats sur une seule machine afin que plusieurs hôtes puissent les utiliser.

Procédure

1. Connectez-vous au Shell ESXi et obtenez les privilèges racine.
2. Passez au répertoire `/etc/vmware/hostd/`.
3. Utilisez un éditeur de texte pour ouvrir le fichier `config.xml` et trouver le segment XML suivant :

   ```
   <ssl>
   <!-- The server private key file -->
   <privateKey>/etc/vmware/ssl/rui.key</privateKey>
   <!-- The server side certificate file -->
   <certificate>/etc/vmware/ssl/rui.crt</certificate>
   </ssl>
   ```

4. Remplacez `/etc/vmware/ssl/rui.key` par le chemin absolu du fichier de clé privée que vous avez reçu de la part de votre autorité de certification approuvée.

   Ce chemin peut se trouver sur l'hôte ou une machine centralisée sur laquelle vous stockez les certificats et clés de votre entreprise.

   Remarque Ne touchez pas aux balises XML `<privateKey>` et `</privateKey>`.

5 Remplacez `/etc/vmware/ssl/rui.crt` par le chemin absolu du fichier de certificat que vous avez reçu de la part de votre autorité de certification approuvée.

AVERTISSEMENT Ne supprimez pas les fichiers d'origine `rui.key` et `rui.crt`. L'hôte utilise ces fichiers.

6 Enregistrez les modifications et fermez le fichier.

7 Redémarrez le processus hôte :

```
/etc/init.d/hostd restart
```

Modifier les paramètres de sécurité pour un service Proxy Web

Vous pouvez modifier la configuration de sécurité afin que des services individuels soient directement accessibles via des connexions HTTP.

Procédure

1 Connectez-vous au Shell ESXi et obtenez les privilèges root. **[]**

2 Passez au répertoire `/etc/vmware/hostd/`.

3 Utilisez un éditeur de texte pour ouvrir le fichier `proxy.xml`.

Le fichier comporte généralement les éléments suivants :

```
<ConfigRoot>
<EndpointList>
<_length>10</_length>
<_type>vim.ProxyService.EndpointSpec[]</_type>
<e id="0">
<_type>vim.ProxyService.LocalServiceSpec</_type>
<accessMode>httpsWithRedirect</accessMode>
<port>8309</port>
<serverNamespace>/</serverNamespace>
</e>
<e id="1">
<_type>vim.ProxyService.LocalServiceSpec</_type>
<accessMode>httpAndHttps</accessMode>
<port>8309</port>
<serverNamespace>/client/clients.xml</serverNamespace>
</e>
<e id="2">
<_type>vim.ProxyService.LocalServiceSpec</_type>
<accessMode>httpAndHttps</accessMode>
<port>12001</port>
<serverNamespace>/ha-nfc</serverNamespace>
</e>
<e id="3">
<_type>vim.ProxyService.NamedPipeServiceSpec</_type>
<accessMode>httpsWithRedirect</accessMode>
<pipeName>/var/run/vmware/proxy-mob</pipeName>
<serverNamespace>/mob</serverNamespace>
</e>
<e id="4">
<_type>vim.ProxyService.LocalServiceSpec</_type>
<accessMode>httpAndHttps</accessMode>
<port>12000</port>
```

```
<serverNamespace>/nfc</serverNamespace>
</e>
<e id="5">
<_type>vim.ProxyService.LocalServiceSpec</_type>
<accessMode>httpsWithRedirect</accessMode>
<port>8307</port>
<serverNamespace>/sdk</serverNamespace>
</e>
<e id="6">
<_type>vim.ProxyService.NamedPipeTunnelSpec</_type>
<accessMode>httpOnly</accessMode>
<pipeName>/var/run/vmware/proxy-sdk-tunnel</pipeName>
<serverNamespace>/sdkTunnel</serverNamespace>
</e>
<e id="7">
<_type>vim.ProxyService.LocalServiceSpec</_type>
<accessMode>httpsWithRedirect</accessMode>
<port>8308</port>
<serverNamespace>/ui</serverNamespace>
</e>
<e id="8">
<_type>vim.ProxyService.LocalServiceSpec</_type>
<accessMode>httpsOnly</accessMode>
<port>8089</port>
<serverNamespace>/vpxa</serverNamespace>
</e>
<e id="9">
<_type>vim.ProxyService.LocalServiceSpec</_type>
<accessMode>httpsWithRedirect</accessMode>
<port>8889</port>
<serverNamespace>/wsman</serverNamespace>
</e>
</EndpointList>
</ConfigRoot>
```

4 Modifiez les paramètres de sécurité, si nécessaire.

Par exemple, vous voulez peut-être modifier les entrées pour les services utilisant HTTPS afin d'ajouter l'option d'accès HTTP.

Option	Description
e id	Numéro d'ID pour la balise de serveur ID XML. Les numéros d'ID doivent être uniques dans la zone HTTP.
_type	Nom du service que vous transférez.
accessmode	Formes de communications autorisées par le service. Les valeurs acceptées sont notamment : ■ httpOnly : le service est uniquement accessible sur des connexions HTTP de texte brut. ■ httpsOnly : le service est uniquement accessible sur des connexions HTTPS. ■ httpsWithRedirect : le service est uniquement accessible sur des connexions HTTPS. Les requêtes sur HTTP sont redirigées sur l'URL HTTPS appropriée. ■ httpAndHttps : le service est uniquement accessible sur des connexions HTTPS et HTTP.

Option	Description
port	Numéro de port assigné au service. Vous pouvez assigner un numéro de port différent au service.
serverNamespace	Espace de nom du serveur qui fournit ce service, par exemple `/sdk` ou `/mob`.

5 Enregistrez les modifications et fermez le fichier.

6 Redémarrez le processus `hostd` :

```
/etc/init.d/hostd restart
```

Mode verrouillage

6

Pour augmenter le niveau de sécurité des hôtes ESXi, vous pouvez les placer en mode verrouillage.

Quand vous activez le mode verrouillage, aucun utilisateur autre que `vpxuser` n'a d'autorisations d'authentification, ni ne peut exécuter des opérations directement par rapport à l'hôte. Le mode de verrouillage force l'exécution de toutes les opérations via vCenter Server.

Lorsqu'un hôte est en mode de verrouillage, vous ne pouvez pas exécuter des commandes CLI vSphere à partir d'un serveur d'administration, d'un script ou d'un vMA par rapport à l'hôte. Les outils logiciels et de gestion externes peuvent ne pas pouvoir récupérer ou modifier les informations de l'hôte ESXi.

Remarque L'utilisateur racine est toujours autorisé à ouvrir une session sur l'interface DCUI quand le mode verrouillage est activé.

L'activation ou non du mode de verrouillage affecte les types d'utilisateurs autorisés à accéder aux services d'hôte, mais n'affecte pas la disponibilité de ces services. En d'autres termes, si les services Shell ESXi, SSH ou DCUI (Direct Console User Interface) sont activés, ils continueront de s'exécuter, que l'hôte soit ou non en mode verrouillage.

Vous pouvez activer le mode de verrouillage en utilisant l'assistant Ajouter hôte pour ajouter un hôte à vCenter Server, vSphere Client pour gérer un hôte ou l'interface utilisateur de console directe.

Remarque Si vous activez ou désactivez le mode de verrouillage en utilisant l'interface DCUI (Direct Console User Interface), les autorisations des utilisateurs et des groupes sur l'hôte sont supprimées. Pour conserver ces autorisations, vous devez activer et désactiver le mode de verrouillage en utilisant vSphere Client connecté à vCenter Server.

Le mode de verrouillage est disponible uniquement sur les hôtes ESXi qui ont été ajoutés à vCenter Server.

Ce chapitre aborde les rubriques suivantes :

Comportement du mode verrouillage

Activer le mode verrouillage détermine quels utilisateurs sont autorisés à accéder aux services hôtes.

Les utilisateurs qui étaient connectés au Shell ESXi avant l'activation du mode de verrouillage restent connectés et peuvent exécuter des commandes. Toutefois, ces utilisateurs ne peuvent pas désactiver le mode de verrouillage. Aucun autre utilisateur, notamment l'utilisateur racine et les utilisateurs ayant le rôle Administrateur sur l'hôte, ne peut utiliser le Shell ESXi pour se connecter à un hôte verrouillé.

Les utilisateurs ayant les privilèges d'administrateur sur le système vCenter Server peuvent utiliser vSphere Client pour désactiver le mode de verrouillage pour les hôtes gérés par le système vCenter Server. Les utilisateurs racine et les utilisateurs ayant le rôle Administrateur peuvent toujours se connecter directement à l'hôte en utilisant l'interface DCUI (Direct Console User Interface) pour désactiver le mode de verrouillage. Si l'hôte n'est pas géré par vCenter Server ou s'il est inaccessible, vous devez installer ESXi.

Remarque Le mode de verrouillage ne s'applique pas aux utilisateurs racine qui se connectent en utilisant des clés autorisées. Lorsque vous utilisez un fichier de clés autorisées pour authentifier les utilisateurs racine, ces derniers ne sont pas empêchés d'accéder à un hôte avec SSH lorsque l'hôte est verrouillé.

Différents services sont mis à la disposition de différents types d'utilisateurs lorsque l'hôte fonctionne en mode verrouillage, ce qui n'est pas le cas lorsque l'hôte fonctionne en mode normal.

Tableau 6-1. Comportement du mode verrouillage

Service	Mode normal	Mode verrouillage
vSphere WebServices API	Tous les utilisateurs, basés sur les autorisations ESXi	vCenter seulement (vpxuser)
Fournisseurs CIM	Utilisateurs racine et utilisateurs disposant du rôle administrateur sur l'hôte	vCenter seulement (ticket)
Interface utilisateur de la console directe (DCUI)	Utilisateurs racine et utilisateurs disposant du rôle administrateur sur l'hôte	Utilisateurs Root
ESXi Shell	Utilisateurs racine et utilisateurs disposant du rôle administrateur sur l'hôte	Aucun utilisateur
SSH	Utilisateurs racine et utilisateurs disposant du rôle administrateur sur l'hôte	Aucun utilisateur

Configurations du mode verrouillage

Vous pouvez activer ou désactiver l'accès distant et local au Shell ESXi pour créer différentes configurations de mode verrouillage.

Le tableau suivant répertorie les services qui sont activés pour trois configurations types.

Avertissement Si vous avez perdu l'accès à vCenter Server lors du fonctionnement en mode verrouillage total, vous devez réinstaller ESXi pour accéder de nouveau à l'hôte.

Tableau 6-2. Configurations du mode verrouillage

Service	Configuration par défaut	Configuration recommandée	Configuration verrouillage total
Verrouillage	Désactivé	Activé	Activé
ESXi Shell	Désactivé	Désactivé	Désactivé

Tableau 6-2. Configurations du mode verrouillage (suite)

Service	Configuration par défaut	Configuration recommandée	Configuration verrouillage total
SSH	Désactivé	Désactivé	Désactivé
Interface utilisateur de la console directe (DCUI)	Activé	Activé	Désactivé

Activation du mode verrouillage à l'aide de vSphere Client

Vous pouvez activer le mode verrouillage afin d'imposer l'apport des modifications de configuration via vCenter Server. Vous pouvez également activer ou désactiver ce mode via l'interface utilisateur de console directe (DCUI).

Procédure

1 Connectez-vous à un système vCenter Server en utilisant vSphere Client.

2 Sélectionnez l'hôte dans le panneau d'inventaire.

3 Cliquez sur l'onglet **[Configuration]** , puis cliquez sur **[Profil de sécurité]** .

4 Cliquez sur le lien **[Modifier]** à côté du mode de verrouillage.

La boîte de dialogue de mode verrouillage apparaît.

5 Sélectionnez **[Activer le mode verrouillage]** .

6 Cliquez sur **[OK]** .

Activation du mode verrouillage à partir de l'interface utilisateur de la console directe

Vous pouvez activer le mode verrouillage depuis l'interface utilisateur de la console directe (DCUI).

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 devez activer et désactiver le mode verrouillage en utilisant vSphere Client connecté à vCenter Server.

Procédure

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

2 Accédez au paramètre **[Configurer le mode verrouillage]** et appuyez sur Entrée.

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

Utilisation du Shell ESXi

Le Shell ESXi (anciennement mode support technique ou TSM) est désactivé par défaut sur ESXi. Vous pouvez activer l'accès local et distant au shell si nécessaire.

Activez le Shell ESXi uniquement à des fins de dépannage. Le Shell ESXi peut être activé et désactivé, que l'hôte fonctionne en mode verrouillage ou non.

Shell ESXi	Activez ce service pour accéder localement au Shell ESXi.
SSH	Activez ce service pour accéder à distance au Shell ESXi en utilisant SSH.
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 vSphere Client ou en activant le Shell ESXi.

L'utilisateur racine et les utilisateurs disposant du rôle d'administrateur peuvent accéder au Shell ESXi. Les utilisateurs du groupe Active Directory ESX Admins reçoivent automatiquement le rôle d'administrateur.

Remarque N'activez pas le Shell ESXi tant que cela n'est pas nécessaire. Quand le shell est activé, toutes les personnes connectées ont un total contrôle sur l'hôte.

Connexion au ESXi Shell pour une opération de dépannage

Vous pouvez accomplir les tâches de configuration d'ESXi via vSphere Client ou à l'aide de vSphere CLI. Connectez-vous au Shell ESXi (anciennement mode support technique ou TSM) uniquement à des fins de dépannage.

Procédure

1 Connectez-vous au Shell ESXi en utilisant l'une des méthodes suivantes.

- Si vous avez un accès direct à l'hôte, appuyez sur la combinaison de touches Alt+F2 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.

Utiliser vSphere Client pour activer l'accès au Shell ESXi

Utilisez vSphere Client pour activer l'accès local et distant au Shell ESXi

Procédure

1 Connectez-vous à un système vCenter Server en utilisant vSphere Client.

2 Sélectionnez l'hôte dans le panneau d'inventaire.

3 Cliquez sur l'onglet **[Configuration]** , puis cliquez sur **[Profil de sécurité]** .

4 Dans la section Services, cliquez sur **[Propriétés]** .

5 Sélectionnez un service dans la liste.

- Shell ESXi
- SSH
- IU de Direct Console

6 Cliquez sur **[Options]** et sélectionnez **[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]** .

9 (Facultatif) Définissez le délai d'attente du Shell ESXi.

La valeur par défaut pour le Shell ESXi est 0 (désactivé).

Le délai d'attente correspond au nombre de minutes qui s'écoulent avant que vous deviez vous connecter après l'activation du Shell ESXi. Lorsque le délai est écoulé, le shell est désactivé si vous ne vous êtes pas connecté.

Remarque Si vous avez ouvert une session au moment de l'expiration de ce délai, elle restera ouverte. Toutefois, le Shell ESXi est désactivé pour empêcher d'autres utilisateurs de se connecter.

---

a Sélectionnez l'hôte dans l'inventaire et cliquez sur l'onglet **[Configuration]** .

b Sous Logiciel, sélectionnez **[Paramètres avancés]** .

c Dans le panneau de gauche, sélectionnez **[UserVars]** .

d Dans le champ UserVars.ESXiShellTimeOut, entrez la valeur du délai d'attente.

e Cliquez sur **[OK]** .

Utiliser l'interface utilisateur de la console directe (DCUI) pour activer l'accès au Shell ESXi

L'interface utilisateur de la console directe (DCUI) vous permet d'interagir avec l'hôte localement en utilisant des menus textuels. Vous pouvez utiliser l'interface utilisateur de la console directe pour activer l'accès local et distant au Shell ESXi.

Remarque Les modifications apportées à l'hôte en utilisant l'interface utilisateur de la console directe, vSphere Client, ESXCLI ou d'autres Outils d'administration sont réservées à un stockage permanent toutes les heures ou lors d'un arrêt dans les règles. Les modifications pourraient être perdues si l'hôte échoue avant qu'elles ne soient réservées.

Procédure

1 Depuis 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 le shell ESXi
- Activer SSH

4 Appuyez sur Entrée pour activer le service souhaité.

5 (Facultatif) Définissez le délai d'attente du Shell ESXi.

La valeur par défaut pour le Shell ESXi est 0 (désactivé).

Le délai d'attente correspond au nombre de minutes qui s'écoulent avant que vous deviez vous connecter après l'activation du Shell ESXi. Lorsque le délai est écoulé, le shell est désactivé si vous ne vous êtes pas connecté.

Remarque Si vous avez ouvert une session au moment de l'expiration de ce délai, elle restera ouverte. Toutefois, le Shell ESXi est désactivé pour empêcher d'autres utilisateurs de se connecter.

---

a Dans le menu Options de mode de dépannage, sélectionnez **[Modifier le délai d'attente du ESXi Shell]** et appuyez sur Entrée.

b Entrez le délai d'expiration (en minutes).

c Appuyez sur Entrée.

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

Meilleures pratiques pour la sécurité des machines virtuelles et des hôtes 7

Tenez compte des recommandations de base en matière de sécurité lorsque vous créez et configurez des hôtes et des machines virtuelles.

Ce chapitre aborde les rubriques suivantes :

Recommandations destinées aux machines virtuelles

Plusieurs précautions de sécurité sont à prendre dans le cadre de l'évaluation de la sécurité des machines virtuelles et de leur administration.

Installation d'un logiciel anti-virus

Chaque machine virtuelle héberge un système d'exploitation standard ; par conséquent, vous pouvez la protéger contre les virus en installant un logiciel anti-virus. 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 enregistreront 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).

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.

Activation des opérations Copier et Coller entre le système d'exploitation invité et la console distante

Pour effectuer des opérations Copier et Coller entre le système d'exploitation invité et la console distante, vous devez activer ces opérations à l'aide de vSphere Client.

Procédure

1 Ouvrez une session sur un système vCenter Server à l'aide de vSphere Client, et sélectionnez une machine virtuelle.

2 Cliquez sur l'onglet **[Résumé]** et cliquez sur **[Modifier les paramètres]** .

3 Sélectionnez **[Options]** > **[Avancé]** > **[Généralités]** et cliquez sur **[Paramètres de configuration]** .

4 Cliquez sur **[Ajouter ligne]** et tapez les valeurs suivantes dans les colonnes de nom et de valeur.

Nom	Valeur
isolation.tools.copy.disable	false
isolation.tools.paste.disable	false

Ces options écrasent les valeurs entrées dans Panneau de configuration de VMware Tools, sur le système d'exploitation invité.

5 Cliquez sur **[OK]** pour fermer la boîte de dialogue de paramètres de configuration, puis sur **[OK]** pour fermer la boîte de dialogue de propriétés de machine virtuelle.

6 Redémarrez la machine virtuelle.

Retrait des périphériques matériels inutiles

Les utilisateurs et les processus ne disposant pas de privilèges d'accès sur une machine virtuelle peuvent connecter ou déconnecter des périphériques matériels (adaptateurs réseau et lecteurs de CD-ROM, par exemple). Par conséquent, le retrait des périphériques matériels inutiles peut empêcher la survenue d'attaques.

Les pirates peuvent utiliser ce moyen pour enfreindre la sécurité des machines virtuelles, via différentes méthodes. Par exemple, un pirate possédant un accès à une machine virtuelle peut reconnecter un lecteur de CD-ROM déconnecté et accéder aux informations sensibles figurant sur le support inséré dans le lecteur ; il peut également déconnecter un adaptateur réseau afin d'isoler la machine virtuelle de son réseau, entraînant une attaque de déni de service (DoS).

Il est recommandé, pour des raisons de sécurité, d'utiliser les commandes de l'onglet vSphere Client **[Configuration]** pour supprimer tous les périphériques matériels inutiles. Cette mesure renforce la sécurité des machines virtuelles ; toutefois, elle n'est pas recommandée si vous pensez devoir ultérieurement remettre un périphérique inutilisé en service.

Interdiction pour les utilisateurs ou les processus de machines virtuelles de déconnecter les périphériques

Si vous ne souhaitez pas supprimer en permanence un périphérique, vous pouvez empêcher un utilisateur ou un processus de machine virtuelle de déconnecter ce périphérique du système d'exploitation invité.

Procédure

1 Ouvrez une session sur un système vCenter Server au moyen de vSphere Client.

2 Sélectionnez la machine virtuelle dans l'inventaire.

3 Cliquez sur l'onglet **[Résumé]** et cliquez sur **[Modifier les paramètres]** .

4 Sélectionnez **[Options] > [Options générales]** et enregistrez le chemin qui s'affiche dans la zone de texte **[Fichier de configuration de la machine virtuelle]** .

5 Connectez-vous à Shell ESXi et obtenez les privilèges racine.

6 Changez les répertoires afin d'accéder au fichier de configuration de la machine virtuelle, dont vous avez enregistré le chemin dans Étape 4.

   Les fichiers de configuration des machines virtuelles se situent dans l'inventaire `/vmfs/volumes/`*`banque de données`*, où *banque de données* correspond au nom du périphérique de stockage sur lequel résident les fichiers de la machine virtuelle. Par exemple, si le fichier de configuration de la machine virtuelle indiqué dans la boîte de dialogue des propriétés de machine virtuelle est `[vol1]vm-finance/vm-finance.vmx`, accédez au répertoire suivant :

   ```
   /vmfs/volumes/vol1/vm-finance/
   ```

7 Utilisez un éditeur de texte pour ajouter la ligne suivante au fichier `.vmx` file, où *device_name* correspond au nom du périphérique à protéger (par exemple : `ethernet1`).

   ```
   device_name.allowGuestConnectionControl = "false"
   ```

   Remarque Par défaut, Ethernet 0 est configuré de façon à empêcher la déconnexion de périphériques. Le seul motif de modification de cette configuration se présente lorsqu'un administrateur précédent a défini *`device_name`*`.allowGuestConnectionControl` sur `true`.

8 Enregistrez les modifications et fermez le fichier.

9 Dans vSphere Client, cliquez avec le bouton droit sur la machine virtuelle et sélectionnez **[Power Off]** .

10 Cliquez avec le bouton droit sur la machine virtuelle et sélectionnez **[Mettre sous tension]** .

Limitation des opérations d'écriture du système d'exploitation invité dans la mémoire de l'hôte

Les processus du système d'exploitation invité envoient des messages d'information à l'hôte via VMware Tools. Si la quantité de données stockées sur l'hôte pour ces messages était illimitée, ce flux de données risquerait de favoriser les attaques de déni de service (DoS).

Les messages d'information envoyés par les processus du système d'exploitation invité sont appelés `setinfo` et contiennent généralement des paires de données nom/valeur qui définissent les caractéristiques des machines virtuelles ou des identifiants stockés sur l'hôte (par exemple `ipaddress=10.17.87.224`). La taille du fichier de configuration contenant ces paires nom/valeur est limitée à 1 Mo : cela empêche les pirates de lancer des attaques de déni de service (DoS) via l'écriture de logiciels imitant VMware Tools et le remplissage de la mémoire de l'hôte à l'aide de données de configuration arbitraires, ce qui a pour effet de consommer l'espace requis par les machines virtuelles.

Si vous avez besoin de plus de 1 Mo de stockage pour les paires nom/valeur, vous pouvez modifier la valeur de ce paramètre. Vous pouvez également empêcher les processus du système d'exploitation invité d'écrire des paires nom/valeur dans le fichier de configuration.

Modification de la limite de mémoire variable du système d'exploitation invité

Vous pouvez augmenter la limite de mémoire variable du système d'exploitation invité si de grandes quantités d'informations personnalisées sont stockées dans le fichier de configuration.

Procédure

1 Ouvrez une session sur un système vCenter Server au moyen de vSphere Client.

2 Sélectionnez la machine virtuelle dans l'inventaire.

3 Cliquez sur l'onglet **[Résumé]** et cliquez sur **[Modifier les paramètres]** .

4 Sélectionnez **[Options]** > **[Avancé]** > **[Généralités]** et cliquez sur **[Paramètres de configuration]** .

5 Si l'attribut de limite de taille n'y figure pas, vous devez l'ajouter.

   a Cliquez sur **[Ajouter ligne]** .

   b Dans la colonne de nom, tapez `tools.setInfo.sizeLimit`.

   c Dans la colonne de valeur, tapez `Number of Bytes`.

   Si l'attribut de limite de taille existe, modifiez-le pour qu'il indique les limites appropriées.

6 Cliquez sur **[OK]** pour fermer la boîte de dialogue de paramètres de configuration, puis sur **[OK]** pour fermer la boîte de dialogue de propriétés de machine virtuelle.

Interdiction d'envoi de messages de configuration à l'hôte par les processus du système d'exploitation invité

Vous pouvez empêcher les invités d'écrire des paires nom/valeur dans le fichier de configuration. Cette mesure est appropriée lorsque les systèmes d'exploitation invités ne doivent pas être autorisés à modifier les paramètres de configuration.

Procédure

1 Ouvrez une session sur un système vCenter Server au moyen de vSphere Client.

2 Sélectionnez la machine virtuelle dans l'inventaire.

3 Cliquez sur l'onglet **[Résumé]** et cliquez sur **[Modifier les paramètres]** .

4 Sélectionnez **[Options]** > **[Avancé]** > **[Généralités]** et cliquez sur **[Paramètres de configuration]** .

5 Cliquez sur **[Ajouter ligne]** et tapez les valeurs suivantes dans les colonnes de nom et de valeur.

   - Dans la colonne de nom : `isolation.tools.setinfo.disable`
   - Dans la colonne de valeur : `true`

6 Cliquez sur **[OK]** pour fermer la boîte de dialogue de paramètres de configuration, puis sur **[OK]** pour fermer la boîte de dialogue de propriétés de machine virtuelle.

Configuration des niveaux de journalisation applicables au système d'exploitation invité

Les machines virtuelles peuvent consigner des informations de dépannage dans un fichier journal stocké sur le volume VMFS. Les utilisateurs et les processus de la machine virtuelle peuvent effectuer un nombre trop élevé de consignations (intentionnellement ou accidentellement) ; de grandes quantités de données sont donc incluses dans ce fichier journal. A terme, cela risque d'entraîner une forte consommation sur le système de fichiers, jusqu'à provoquer un déni de service.

Pour éviter ce problème, vous pouvez modifier les paramètres de journalisation applicables aux systèmes d'exploitation invités des machines virtuelles. Ces paramètres peuvent limiter la taille totale des fichiers journaux, ainsi que leur nombre. Normalement, un nouveau fichier journal est créé lors de chaque redémarrage d'hôte ; par conséquent, le fichier peut devenir très volumineux. Vous pouvez paramétrer une création de fichier journal plus fréquente en limitant sa taille maximale. VMware recommande de sauvegarder 10 fichiers journaux, avec une taille maximale de 100 Ko par fichier. En effet, ces valeurs sont suffisantes pour la collecte des informations requises en cas de débogage.

Lors de chaque entrée dans le journal, la taille de ce dernier est vérifiée. Si cette taille dépasse la limite fixée, l'entrée suivante sera enregistrée dans un nouveau fichier journal. Dès que le nombre maximal de fichiers journaux est atteint, le fichier le plus ancien est supprimé. Une attaque de déni de service (DoS) ignorant ces limites pourrait être tentée via l'enregistrement d'une énorme entrée de journal ; mais puisque la taille des entrées est limitée à 4 Ko, la taille d'un fichier journal ne peut jamais dépasser la limite configurée de plus de 4 Ko.

Limitation du nombre et de la taille des fichiers journaux

Pour éviter que les utilisateurs et les processus de machine virtuelle n'envoient massivement des messages dans le fichier journal (ce qui risquerait d'entraîner une attaque de déni de service), vous pouvez limiter le nombre et la taille des fichiers journaux créés par ESXi.

Procédure

1 Connectez-vous à un système vCenter Server en utilisant vSphere Client.

2 Cliquez sur l'onglet **[Résumé]** et cliquez sur **[Modifier les paramètres]** .

3 Sélectionnez **[Options]** > **[Options générales]** et enregistrez le chemin qui s'affiche dans la zone de texte **[Fichier de configuration de la machine virtuelle]** .

4 Connectez-vous à ESXi Shell et obtenez les privilèges racine.

5 Changez les répertoires afin d'accéder au fichier de configuration de la machine virtuelle, dont vous avez enregistré le chemin dans Étape 3.

   Les fichiers de configuration des machines virtuelles se situent dans l'inventaire `/vmfs/volumes/`*`banque de données`*, où *banque de données* correspond au nom du périphérique de stockage sur lequel résident les fichiers de la machine virtuelle. Par exemple, si le fichier de configuration de la machine virtuelle indiqué dans la boîte de dialogue des propriétés de machine virtuelle est `[vol1]vm-finance/vm-finance.vmx`, accédez au répertoire suivant :

   ```
   /vmfs/volumes/vol1/vm-finance/
   ```

6 Pour limiter la taille du fichier journal, utilisez un éditeur de texte pour ajouter la ligne suivante au fichier `.vmx` ou la modifier (où *maximum_size* correspond à la taille maximale du fichier, exprimée en octets).

   ```
   log.rotateSize=maximum_size
   ```

   Par exemple, pour limiter la taille à environ 100 Ko, entrez **`100000`**.

7 Pour limiter le nombre de fichiers journaux, utilisez un éditeur de texte pour ajouter la ligne suivante au fichier `.vmx` ou la modifier (où *number_of_files_to_keep* correspond au nombre de fichiers conservés par le serveur).

   ```
   log.keepOld=number_of_files_to_keep
   ```

   Par exemple, pour conserver 10 fichiers journaux et commencer à supprimer les plus anciens au fur et à mesure que de nouveaux fichiers sont créés, entrez **`10`**.

8 Enregistrez les modifications et fermez le fichier.

Désactivation de la journalisation pour le système d'exploitation invité

Si vous choisissez de ne pas consigner les informations de dépannage dans un fichier journal de machine virtuelle stocké sur le volume VMFS, vous pouvez mettre hors tension la journalisation.

Si vous désactivez la journalisation pour le système d'exploitation invité, vous devez savoir que vous ne pourrez peut-être pas disposer des informations de fichier journal requises pour le dépannage. Par ailleurs, si la journalisation a été désactivée, VMware n'assure pas de support technique pour les problèmes survenant sur les machines virtuelles.

Procédure

1 Ouvrez une session sur un système vCenter Server à l'aide de vSphere Client, puis sélectionnez la machine virtuelle souhaitée dans l'inventaire.

2 Cliquez sur l'onglet **[Résumé]** et cliquez sur **[Modifier les paramètres]** .

3 Cliquez sur l'onglet **[Options]** et, dans la liste des options sous Avancé, sélectionnez **[Général]** .

4 Dans paramètres, désélectionnez **[Activer journalisation]** .

5 Cliquez sur **[OK]** pour fermer la boîte de dialogue de propriétés de machine virtuelle.

Trafic de la journalisation de la tolérance aux pannes

Lorsque vous activez Fault Tolerance (FT), VMware vLockstep capture les entrées et les événements qui se produisent sur une machine virtuelle principale et les transmet à la machine virtuelle secondaire qui est exécutée 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 de l'intercepteur ». Par exemple, vous pouvez utiliser un réseau privé pour le trafic de la journalisation de la tolérance aux pannes.

Considérations relatives à la sécurité d'Auto Deploy

Pour protéger au mieux votre environnement, vous devez connaître les risques de sécurité potentiels lorsque vous utilisez Auto Deploy avec des profils d'hôte.

Dans la plupart des cas, les administrateurs configurent Auto Deploy pour provisionner des hôtes cibles non seulement avec une image, mais aussi avec un profil d'hôte. Le profil d'hôte contient des informations de configuration telles que les paramètres réseau ou d'authentification. Les profils d'hôte peuvent être configurés pour inviter l'utilisateur à fournir des informations lors du premier démarrage. Les informations fournies par l'utilisateur sont sauvegardées dans un fichier de réponses. Le profil d'hôte et le fichier de réponses (le cas échéant) sont inclus dans l'image de démarrage qu'Auto Deploy télécharge sur une machine.

- Le mot de passe administrateur (racine) et les mots de passe utilisateur qui sont inclus dans le profil d'hôte et le fichier de réponses sont cryptés en MD5. Tous les autres mots de passe associés aux profils d'hôte sont en clair.
- Utilisez vSphere Authentication Service pour paramétrer Active Directory afin d'éviter d'exposer le mot de passe d'Active Directory. Si vous paramétrez Active Directory en utilisant des profils d'hôte, les mots de passe sont protégés.
- Les fichiers qui contiennent les informations sur le profil d'hôte et le fichier de réponses sont stockés sur disque sous une forme assombrie. Les fichiers peuvent être récupérés uniquement en tant que fichier `waiter.tgz` généré pour chaque hôte. Les fichiers bruts ne sont pas accessibles via le serveur Web. Cependant, il est possible qu'un code malveillant prétende être un hôte et télécharge le fichier `waiter.tgz` de l'hôte qui contient des informations qui peuvent être utilisées pour compromettre l'hôte.

Pour réduire considérablement les risques de sécurité d'Auto Deploy, isolez complètement le réseau où Auto Deploy est utilisé.

Pour plus d'informations sur Auto Deploy, consultez les informations relatives à Auto Deploy qui font partie de la documentation *Installation et configuration de vSphere*. Pour plus d'informations sur les profils d'hôte et les fichiers de réponses, consultez la documentation *Profils d'hôte vSphere*.

Niveau de sécurité et complexité des mots de passe de l'hôte

Par défaut, ESXi utilise le plug-in `pam_passwdqc.so` pour définir les règles que les utilisateurs doivent respecter lors de la création de mots de passe, et pour définir le niveau de sécurité des mots de passe.

Pour déterminer les règles de base à appliquer à tous les mots de passe, configurez le plug-in `pam_passwdqc.so`. Par défaut, ESXi n'impose aucune limitation au niveau du mot de passe racine. Toutefois, lorsque des utilisateurs autres que l'utilisateur racine tentent de changer leurs mots de passe, les mots de passe choisis doivent correspondre aux règles de base définies par `pam_passwdqc.so`.

Un mot de passe valide doit contenir une combinaison du plus grand nombre possible de classes de caractères. Les classes de caractères comprennent les lettres minuscules, les majuscules, les chiffres et les caractères spéciaux (traits de soulignement ou tirets, par exemple).

Remarque Lorsque le nombre de classes de caractères est compté, le plug-in ne compte pas les lettres majuscules utilisées en tant que premier caractère du mot de passe, ni les chiffres utilisés en tant que dernier caractère.

Pour configurer la complexité des mots de passe, vous pouvez modifier la valeur par défaut des paramètres suivants :

- *retry* correspond au nombre de demandes de nouveau mot de passe à l'utilisateur si le mot de passe n'est pas suffisamment long.
- *N0* représente le nombre de caractères requis pour un mot de passe qui utilise uniquement des caractères provenant d'une seule classe de caractères. Par exemple, le mot de passe ne contient que des lettres minuscules.
- *N1* représente le nombre de caractères requis pour un mot de passe qui utilise des caractères provenant de deux classes de caractères.
- *N2* est utilisé pour les phrases de passe. ESXi nécessite trois mots pour une phrase de passe. Chaque mot doit avoir une longueur comprise entre 8 et 40 caractères.
- *N13* représente le nombre de caractères requis pour un mot de passe qui utilise des caractères provenant de trois classes de caractères.
- *N14* représente le nombre de caractères requis pour un mot de passe qui utilise des caractères provenant de quatre classes de caractères.
- *match* représente le nombre de caractères autorisés dans une chaîne de l'ancien mot de passe. Si le plug-in `pam_passwdqc.so` trouve une chaîne réutilisée de cette longueur ou plus longue, il la supprime du test et utilise uniquement les autres caractères.

Si vous affectez à ces options la valeur `-1`, cela indique au plug-in `pam_passwdqc.so` qu'il doit ignorer cette limitation.

Si vous affectez à ces options la valeur `disabled`, cela indique au plug-in `pam_passwdqc.so` qu'il doit disqualifier les mots de passe contenant cette caractéristique. Les valeurs utilisées doivent figurer par ordre décroissant, à l'exception de `-1` et de `disabled`.

Remarque Le plug-in `pam_passwdqc.so` utilisé dans Linux offre davantage de paramètres que ceux pris en charge pour ESXi.

Pour plus d'informations sur le plug-in `pam_passwdqc.so`, consultez la documentation Linux.

Modification de la complexité des mots de passe par défaut pour le plug-in pam_passwdqc.so

Pour déterminer les règles standard à appliquer à tous les mots de passe, configurez le plug-in `pam_passwdqc.so`.

Procédure

1. Connectez-vous au Shell ESXi et obtenez les privilèges root. **[]**
2. Ouvrez le fichier `passwd` avec un éditeur de texte.

   Par exemple, `vi /etc/pam.d/passwd`

3 Modifiez la ligne qui suit.

```
password requisite /lib/security/$ISA/pam_passwdqc.so retry=N min=N0,N1,N2,N3,N4
```

4 Enregistrez le fichier.

Exemple : Modifier /etc/pam.d/passwd

```
password requisite /lib/security/$ISA/pam_passwdqc.so retry=3 min=12,9,8,7,6
```

Avec ces paramètres en place, les critères des mots de passe sont les suivants :

- retry=3 : Un utilisateur a droit à trois tentatives pour entrer un mot de passe suffisant.
- *N0*=12 : Le mot de passe comportant des caractères d'une seule classe doit contenir au moins 12 caractères.
- *N1*=9 : Le mot de passe comportant des caractères de deux classes doit contenir au moins neuf caractères.
- *N2*=8 : La phrase de passe doit contenir des mots d'au moins huit caractères.
- *N3*=7 : Le mot de passe comportant des caractères de trois classes doit contenir au moins sept caractères.
- *N4*=6 : Le mot de passe comportant des caractères des quatre classes doit contenir au moins six caractères.

Index

R

S

T

U

V