Guide de configuration ESX

ESX 4.1

vCenter Serveur 4.1

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-000328-00

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

Copyright © 2009, 2010 VMware, Inc. Tous droits réservés. Ce produit est protégé par les lois américaines et internationales relatives au copyright et à la propriété intellectuelle. Les produits VMware sont protégés par un ou plusieurs brevets répertoriés à l'adresse http://www.vmware.com/go/patents-fr.

VMware est une marque déposée ou une marque de VMware, Inc. aux États-Unis et/ou dans d'autres juridictions. Toutes les autres marques et noms mentionnés sont des marques déposées par leurs propriétaires respectifs.

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

Stockage

Sécurité

À propos de ce guide

Le présent manuel, intitulé *Guide de configurationESX*, contient des informations sur la configuration réseau de VMware® ESX, et y compris les méthodes de création de commutateurs et de ports virtuels et les méthodes de configuration réseau des machines virtuelles, VMware vMotion™ et le stockage IP. Il décrit également la configuration du système de fichiers et de différents types de stockage (iSCSI et Fibre Channel, notamment). Il présente les fonctions de sécurité que contient ESX et les mesures que vous pouvez prendre pour protéger ESX contre les attaques. Il inclut également la liste des commandes de support technique ESX, accompagnées de leurs équivalents VMware vSphere™ Client et d'une description de l'utilitaire `vmkfstools`.

Ces informations concernent ESX 4.1.

Public cible

Ce manuel s'adresse à toute personne devant installer, mettre à niveau ou utiliser ESX. Les informations qu'il contient sont destinées aux administrateurs système Windows ou Linux, familiarisés avec la technologie des machines virtuelles et avec les opérations de centres de données.

Glossaire de VMware Technical Publications

VMware Technical Publications fournit un glossaire des termes qui peuvent éventuellement ne pas vous être familiers. Pour des définitions des termes utilisés dans la documentation technique VMware, rendez-vous sur http://www.vmware.com/support/pubs.

Commentaires sur les documents

VMware prend en considérations vos suggestions pour améliorer sa documentation. Si vous avez des commentaires, envoyez-les à docfeedback@vmware.com

Documentation de vSphere de VMware

La documentation de vSphere VMware est une combinaison de l'ensemble des documentations de VMware vCenter et d'ESX.

Abréviations utilisées dans les figures

Les figures dans ce manuel utilisent les abréviations répertoriées dans Tableau 1.

Tableau 1. Abréviations

Abréviation	Description
base de données	Base de données vCenter Server
banque de données	Stockage pour l'hôte géré

Tableau 1. Abréviations (suite)

Abréviation	Description
dsk#	Disque de stockage pour l'hôte géré
hostn	Hôtes gérés par vCenter Server
SAN	Banque de données de type SAN (Storage Area Network) partagée par les hôtes gérés
tmplt	Modèle
user#	Utilisateur avec autorisations d'accès
VC	vCenter Server
VM#	Machines virtuelles sur un hôte géré

Ressources de support technique et de formation

Les ressources de support technique suivantes sont à votre disposition. Pour accéder à la version actuelle de ce guide et à d'autres guides, allez sur http://www.vmware.com/support/pubs.

Support en ligne et téléphonique

Pour soumettre des demandes d'ordre technique à l'assistance en ligne, consulter les informations concernant vos produits et contrats et inscrire vos produits, rendez-vous sur http://www.vmware.com/support.

Les clients ayant souscrit des contrats de support appropriés peuvent utiliser le support téléphonique pour obtenir une réponse rapide à leurs problèmes prioritaires. Allez sur http://www.vmware.com/support/phone_support.html.

Offres de support

Pour en savoir plus sur la façon dont les offres d'assistance VMware peuvent satisfaire les besoins de votre entreprise, rendez-vous sur http://www.vmware.com/support/services.

VMware Professional Services

Les cours VMware Education Services proposent de nombreux exercices pratiques, des exemples d'étude de cas, ainsi que de la documentation destinée à servir de référence sur site. Les cours sont disponibles sur site, en salle de cours et en ligne et en direct. Pour les programmes pilotes sur site et les meilleures pratiques de mise en œuvre, VMware Consulting Services propose des offres destinées à vous aider à évaluer, planifier, élaborer et gérer votre environnement virtuel. Pour accéder aux informations sur les classes de formation, les programmes de certification et les services-conseil, rendez-vous sur http://www.vmware.com/services.

Présentation de la configuration ESX 1

Ce manuel décrit les tâches à exécuter pour configurer le réseau hôte, le stockage et la sécurité ESX. Par ailleurs, il contient des descriptions et des recommandations qui vous aideront à bien comprendre ces tâches et la méthode de déploiement d'un hôte répondant à vos besoins.

Avant d'utiliser ces informations, lisez la section de *présentation de vSphere* pour obtenir la description de l'architecture système et des périphériques (physiques et virtuels) qui composent les systèmes vSphere.

Cette introduction résume le contenu du présent manuel.

Mise en réseau

Les informations réseau permettent de comprendre les concepts liés aux réseaux physiques et virtuels, les tâches de base à exécuter pour configurer les connexions réseau de votre hôte ESX, ainsi que les concepts et les tâches liés aux réseaux avancés.

Stockage

Les informations sur le stockage permettent de bien comprendre les notions de base liées au stockage et les tâches de base à exécuter pour configurer et gérer le stockage de votre hôte ESX. Elles décrivent également la méthode de mappage de périphérique brut (RDM).

Sécurité

Les informations sur la sécurité décrivent les mesures de sécurité VMware contenues dans ESX, ainsi que les mesures de protection de votre hôte contre les menaces de sécurité qui pèsent sur lui. Ces mesures incluent l'installation d'un pare-feu, l'utilisation des fonctions de sécurité des commutateurs virtuels, ou encore la configuration d'authentifications ou d'autorisations utilisateur.

Profils d'hôte

Cette section décrit la fonction de profils hôte et son utilisation pour encapsuler la configuration d'un hôte dans son profil. Cette section décrit également la méthode d'application de ce profil hôte à un autre hôte ou cluster, ainsi que la méthode de modification de profil et de vérification de la conformité d'un hôte à un profil donné.

Annexes

Les annexes contiennent des informations spécifiques, très utiles lors de la configuration d'hôtes ESX.

- Commandes de support technique ESX – Décrit les commandes utilisées lors de la configuration d'ESX ; pour l'exécution de ces commandes, vous pouvez utiliser un shell de ligne de commande (SSH, par exemple). Bien que ces commandes soient disponibles, ne les considérez pas comme une interface API utilisable pour la génération de scripts. Ces commandes sont sujettes à modification et VMware ne prend pas en charge les applications et les scripts qui prennent comme base les commandes de configuration ESX. Cette annexe contient les équivalents vSphere Client de ces commandes.
- Utilisation de vmkfstools - Décrit l'utilitaire wmkfstools, qui permet de créer et de manipuler des disques virtuels, des systèmes de fichiers, des volumes logiques et des périphériques de stockage physiques sur les hôtes.

Mise en réseau

Introduction à la mise en réseau 2

Les concepts de base de la mise en réseau ESX et la façon d'installer et de configurer un réseau dans un environnement vSphere sont ici présentés.

Ce chapitre aborde les rubriques suivantes :

Présentation des concepts de mise en réseau

Quelques concepts sont essentiels pour bien comprendre la mise en réseau virtuelle. Si vous débutez avec ESX, il peut s'avérer utile de les consulter.

Un réseau physique est un réseau de machines physiques connectées de sorte qu'elles puissent s'envoyer des données et en recevoir entre elles. ESX de VMware s'exécute sur une machine physique.

Un réseau virtuel est un réseau de machines virtuelles fonctionnant sur une machine physique unique, qui sont connectées logiquement entre elles de sorte qu'elles puissent envoyer des données et en recevoir entre elles. Des machines virtuelles peuvent être connectées à des réseaux virtuels que vous créez lorsque vous ajoutez un réseau.

Un commutateur Ethernet physique gère le trafic du réseau entre les machines sur le réseau physique. un commutateur possède plusieurs ports, et chacun peut être connecté à une machine unique ou à un autre commutateur sur le réseau. Chaque port peut être configuré pour se comporter de certaines manières, selon les besoins de la machine à laquelle il est connecté. Le commutateur connaît les hôtes qui sont connectés à ces ports et utilise ces informations pour acheminer le trafic aux machines physiques appropriées. Les commutateurs constituent le coeur d'un réseau physique. Plusieurs commutateurs peuvent être reliés entre eux pour former des réseaux plus grands.

Un commutateur virtuel, appelé vSwitch, fonctionne de façon similaire à un commutateur Ethernet physique. Il détecte les machines virtuelles qui sont logiquement connectées à chacun de ces ports virtuels et utilise ces informations pour acheminer le trafic aux machines virtuelles appropriées. Un vSwitch peut être connecté à des commutateurs physiques à l'aide d'adaptateurs Ethernet physiques, aussi appelés cartes de liaison montante, afin de joindre des réseaux virtuels à des réseaux physiques. Ce type de connexion est semblable à une connexion de commutateurs physiques entre eux visant à créer un réseau plus grand. Même si un vSwitch fonctionne de façon similaire à un commutateur physique, il ne dispose pas de certaines fonctionnalités avancées du commutateur physique.

Un commutateur distribué vNetwork agit en tant que vSwitch unique sur tous les hôtes associés sur un centre de données. Ceci permet à des machines virtuelles de conserver une configuration réseau cohérente pendant qu'elles migrent sur plusieurs hôtes.

Un dvPort est un port sur un commutateur distribué vNetwork qui se connecte à la console de service ou VMkernel d'un hôte, ou à la carte réseau d'une machine virtuelle.

Un groupes de ports spécifie les options de configuration de ports, telles que les restrictions de bande passante et les stratégies de balisage VLAN pour chaque port membre. Les services de réseau se connectent aux vSwitch via des groupes de port. Les groupes de ports définissent la manière dont s'établit une connexion à un réseau via le vSwitch. Généralement, un vSwitch unique est associé à un ou plusieurs groupes de ports.

Un groupes dvPort est un groupes de ports associé à un commutateur distribué vNetwork et spécifie les options de configuration de ports pour chaque port membre. Les groupes dvPort définissent la manière dont s'établit une connexion à un réseau via le commutateur distribué vNetwork.

L'association NIC se produit lorsque plusieurs cartes de liaison montante sont associées à un vSwitch unique. Une association peut partager la charge de trafic entre des réseaux physiques et virtuels parmi certains ou tous ses membres, ou fournir un basculement passif dans l'éventualité d'une défaillance matérielle ou d'une indisponibilité du réseau.

Les VLAN permettent à un segment LAN physique unique d'être davantage segmenté de sorte que des groupes de ports soient isolés les uns des autres comme s'ils se trouvaient sur des segments physiquement différents. La norme est 802.1Q.

La pile réseau TCP/IP de VMkernel prend en charge iSCSI, NFS et vMotion. Les machines virtuelles exécutent leurs propres piles de système TCP/IP et se connectent au VMkernel au niveau de l'Ethernet via des commutateurs virtuels.

Le stockage IP se réfère à toute forme de stockage utilisant la communication de réseau TCP/IP comme sa fondation. iSCSI peut être utilisé comme banque de données de machine virtuelle, et NFS peut être employé comme banque de données de machine virtuelle ainsi que pour le montage direct de fichiers `.ISO`, présentés comme CD-ROM aux machines virtuelles.

Le délestage de segmentation TCP, ou TSO, permet à une pile TCP/IP d'émettre de très grandes trames (jusqu'à 64 Ko) même si l'unité de transmission maximale (MTU) de l'interface est plus petite. La carte réseau sépare alors la grande trame en trames adaptées à la taille MTU, et ajoute une copie ajustée des en-têtes initiaux TCP/IP.

La migration avec vMotion permet à une machine virtuelle sous tension d'être transférée depuis un hôte ESX vers un autre sans arrêter la machine virtuelle. La fonctionnalité facultative vMotion requiert une clé de licence.

Services de réseau

Un vNetwork propose plusieurs services différents à l'hôte et aux machines virtuelles.

Vous pouvez activer trois types de service de réseau dans ESX :

- Connecter des machines virtuelles au réseau physique et entre elles.
- Connecter des services VMkernel (tels que NFS, iSCSI ou vMotion) au réseau physique.
- Exécuter des services de gestion pour ESX via la console de service. Un port de console de service, paramétré par défaut lors de l'installation, est requis par ESX pour se connecter à un réseau quelconque ou à des services à distance, y compris au vSphere Client. Des ports de console de service supplémentaires peuvent s'avérer nécessaires pour d'autres services, tels que le stockage iSCSI.

Afficher les informations de mise en réseau dans vSphere Client

vSphere Client affiche les informations de mise en réseau générales ainsi que des informations spécifiques aux cartes réseau.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Mise en réseau]** .

3 (Facultatif) Choisissez le type de mise en réseau que vous souhaitez voir.

Option	Description
Commutateur virtuel	Affiche la mise en réseau des commutateurs standard vNetwork sur l'hôte.
commutateur distribué vNetwork	Affiche la mise en réseau des commutateur distribué vNetwork sur l'hôte.

L'option **[Commutateur distribué vNetwork]** apparaît uniquement sur des hôtes connectés à un ou plusieurs commutateurs distribués vNetwork.

Les informations de mise en réseau sont affichées pour chaque commutateur virtuel sur l'hôte.

Afficher les informations de carte réseau dans vSphere Client

Pour chaque carte réseau physique sur l'hôte, vous pouvez afficher des informations, telles que la vitesse, le duplex et les plages IP observées.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** , puis sur **[Adaptateurs réseau]** .

Le panneau de cartes réseau affiche les informations suivantes.

Tableau 2-1. Paramètres de carte réseau

Option	Description
[Périphérique]	Nom de la carte réseau.
[Vitesse]	Vitesse et duplex réels de la carte réseau.
[Configuré]	Vitesse et duplex configurés de la carte réseau.
[Commutateur]	vSwitch ou vDS auquel la carte réseau est associée.
[Plages IP observées]	Adresses IP auxquelles l'adaptateur réseau accède.
[Wake on LAN pris en charge]	Possibilité pour l'adaptateur réseau de prendre en charge la fonction Wake on the LAN.

Gestion de réseau de base avec les commutateurs standard vNetwork 3

Les commutateurs standard vNetwork (vSwitches) gèrent le trafic réseau au niveau de l'hôte dans un environnement vSphere.

Utilisez vSphere Client pour ajouter un réseau reposant sur les catégories qui reflètent les types de services réseau :

- Machines virtuelles
- VMkernel
- Console du service

Ce chapitre aborde les rubriques suivantes :

Commutateurs standard vNetwork

Vous pouvez créer des périphériques réseau abstraits appelés commutateurs standard vNetwork (vSwitch). Un vSwitch peut acheminer du trafic de manière interne entre les machines virtuelles et se connecter à des réseaux externes.

Vous pouvez utiliser les vSwitch pour associer la bande passante de plusieurs adaptateurs réseau et équilibrer le trafic de communications entre eux. Vous pouvez également configurer un vSwitch pour traiter le basculement NIC physique.

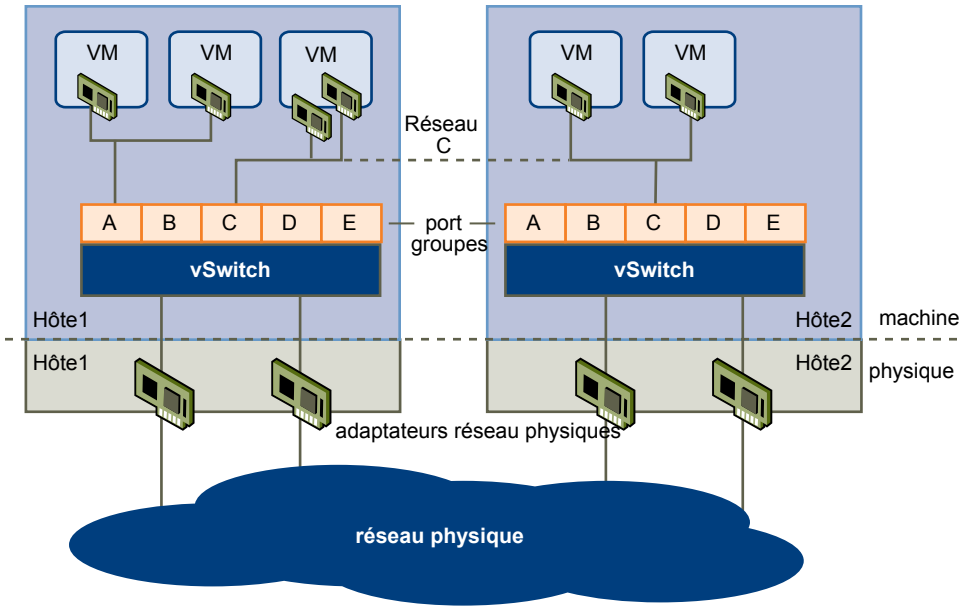
Un vSwitch modélise un commutateur Ethernet physique. Le nombre par défaut de ports logiques pour un vSwitch est 120. Vous pouvez connecter un adaptateur réseau de machine virtuelle à chaque port. Chaque carte de liaison montante associée à un vSwitch emploie un port. Chaque port logique sur le vSwitch est un membre d'un seul groupes de ports. Chaque vSwitch peut également avoir un ou plusieurs groupes de ports qui lui sont affectés. Pour plus d'informations sur le nombre maximum de ports et de groupes de ports autorisés, voir *Maximums de configuration pour vSphere 4.1*.

Si plusieurs machines virtuelles sont connectées au même vSwitch, le trafic réseau entre elles est acheminé localement. Si un adaptateur de liaison montante est connecté au vSwitch, chaque machine virtuelle peut accéder au réseau externe auquel l'adaptateur est connecté.

groupes de ports

Les groupes de ports regroupesnt plusieurs ports sous une configuration commune et fournissent un point d'ancrage stable pour les machines virtuelles qui se connectent à des réseaux étiquetés.

Figure 3-1. Réseau de commutateurs standard vNetwork



Chaque groupes de ports est identifié par une étiquette de réseau, unique à l'hôte actuel. Les étiquettes réseau sont utilisées pour rendre compatible la configuration des machines virtuelles sur les hôtes. Tous les groupes de ports dans le centre de données qui sont physiquement connectés au même réseau (dans le sens que chacun peut recevoir des diffusions des autres) reçoivent le même nom. Au contraire, si deux groupes de ports ne peuvent pas recevoir des diffusions l'un de l'autre, ils ont des étiquettes distinctes.

L'ID de VLAN est facultatif. Elle permet de limiter le trafic du groupes de ports à un segment Ethernet logique dans le réseau physique. Afin que chaque groupes de ports atteigne des groupes de ports situés sur d'autres VLAN, l'ID de VLAN doit être défini sur 4 095. Si vous utilisez des ID de VLAN, vous devez modifier les étiquettes de groupes et les ID de VLAN en même temps afin que les étiquettes représentent correctement la connectivité.

Configuration du groupes de ports pour des machines virtuelles

Vous pouvez ajouter ou modifier un groupes de ports de machines virtuelles à partir de vSphere Client.

L'assistant Ajouter réseau de vSphere Client vous guide à travers les tâches de création de réseau virtuel auquel les machines virtuelles peuvent se connecter, y compris la création d'un vSwitch et les paramètres de configuration de l'étiquette réseau.

Lorsque vous définissez les réseaux de machines virtuelles, envisagez de prendre les mesures pour migrer les machines virtuelles dans le réseau entre les hôtes. Dans ce cas, assurez-vous que les deux hôtes sont dans le même domaine de diffusion, c'est-à-dire dans le même sous-réseau de couche 2.

ESX ne prend pas en charge la migration de machines virtuelles entre des hôtes dans différents domaines de diffusion, car la machine virtuelle migrée nécessite des systèmes et des ressources auxquels elle n'aurait plus accès dans le nouveau réseau. Même si la configuration de votre réseau est définie comme un environnement haute disponibilité ou comprend des commutateurs intelligents qui peuvent résoudre les besoins de la machine virtuelle sur différents réseaux, vous pouvez rencontrer des délais d'attente lors des mises à niveau de la table ARP (Protocole de résolution d'adresse) et de la reprise du trafic réseau pour les machines virtuelles.

Les machines virtuelles atteignent les réseaux physiques via des adaptateurs de liaison montante. Un vSwitch peut transférer des données vers des réseaux externes uniquement quand une ou plusieurs cartes réseau lui sont attachées. Quand deux cartes ou plus sont attachées à un seul vSwitch, elles sont associées de manière transparente.

Ajout d'un groupes de ports de machine virtuelle

Les groupes de ports de machine virtuelle fournissement un réseau pour les machines virtuelles.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Mise en réseau]** .

3 Sélectionnez la vue commutateur virtuel.

Les vSwitch apparaissent dans un aperçu qui comprend une présentation détaillée.

4 Sur le côté droit de la page, cliquez sur **[Ajouter gestion réseau]** .

5 Acceptez le type de connexion par défaut, **[Machines virtuelles]** , puis cliquez sur **[Suivant]** .

6 Sélectionnez **[Créer un commutateur virtuel]** ou l'un des vSwitch existants figurant dans liste et les adaptateurs physiques associés à utiliser pour ce groupes de ports.

Vous pouvez créer un nouveau vSwitch avec ou sans adaptateur Ethernet.

Si vous créez un vSwitch sans adaptateur réseau physique, tout le trafic sur ce vSwitch est confiné sur celui-ci. Aucun autre hôte sur le réseau physique ou les machines virtuelles sur les autres vSwitch ne peut envoyer du trafic sur ce vSwitch. Vous pouvez créer un vSwitch sans adaptateur réseau physique si vous voulez qu'un groupes de machines virtuelles puisse communiquer entre elles, mais avec aucun autre hôte ou machine virtuelle en dehors du groupes.

7 Cliquez sur **[Suivant]** .

8 Dans le groupes Propriétés groupes de ports, entrez une étiquette de réseau qui identifie le groupes de ports que vous créez.

Utilisez des étiquettes réseau pour identifier les connexions compatibles pour la migration communes à deux hôtes ou plus.

9 (Facultatif) Si vous utilisez un VLAN, pour **[ID VLAN]** , entrez un nombre entre 1 et 4 094. Si vous n'utilisez pas un VLAN, laissez ce champ vide.

Si vous entrez 0 ou laissez ce champ vide, le groupes de ports peut uniquement voir le trafic non balisé (non VLAN). Si vous entrez 4 095, le groupes de ports peut voir le trafic sur n'importe quel VLAN tout en laissant les balises VLAN intactes.

10 Cliquez sur **[Suivant]** .

11 Après avoir déterminé que le vSwitch est configuré correctement, cliquez sur **[Terminer]** .

Configuration de réseau VMkernel

Une interface réseau VMkernel est utilisée pour vMotion de VMware, le stockage IP et Fault Tolerance.

Le déplacement d'une machine virtuelle d'un hôte à un autre est appelé migration. vMotion vous permet de migrer des machines virtuelles sous tension sans temps d'arrêt. Votre pile réseau VMkernel doit être configurée correctement pour recevoir vMotion.

Le stockage IP se rapporte au stockage utilisant la communication réseau TCP/IP comme base, qui comprend l'iSCSI, le FCoE et le NFS pour ESX. Comme ces types de stockages reposent sur le réseau, ils peuvent utiliser la même interface VMkernel et le même groupes de ports.

Les services réseau que VMkernel fournit (iSCSI, NFS et vMotion) utilisent un pile TCP/IP dans VMkernel. Cette pile TCP/IP est totalement séparée de la pile TCP/IP utilisée dans la console du service. Chacune des ces piles TCP/IP accède à différents réseaux en connectant un ou plusieurs groupes de ports sur un ou plusieurs vSwitch.

Pile TCP/IP au niveau de VMkernel

La pile réseau TCP/IP VMkernel de VMware fournit la prise en charge réseau de plusieurs manières pour chaque service qu'elle traite.

La pile TCP/IP VMkernel traite iSCSI, NFS et vMotion des manières suivantes.

- iSCSI comme banque de données de machine virtuelle.
- iSCSI pour le montage direct de fichiers `.ISO`, qui sont présentés comme des CD-ROM virtuels aux machines virtuelles.
- NFS comme banque de données de machine virtuelle.
- NFS pour le montage direct de fichiers `.ISO`, qui sont présentés comme des CD-ROM virtuels aux machines virtuelles.
- Migration avec vMotion.
- Journalisation de la tolérance aux pannes.
- Fournit des informations réseau aux cartes matérielles iSCSI dépendantes.

Si vous avez deux cartes réseau iSCSI physiques ou plus, vous pouvez créer plusieurs chemins pour le logiciel iSCSI en configurant les chemins multiples iSCSI. Pour plus d'informations sur le chemins multiples, consultez le *Guide de configuration SAN iSCSI*.

Remarque ESX prend uniquement en charge NFS version 3 sur TCP/IP.

Configuration du réseau VMkernel

Créez un adapteur réseau VMkernel utilisable en tant qu'interface vMotion ou que groupes de ports de stockage d'IP.

Procédure

1. Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.
2. Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Mise en réseau]** .
3. Dans la vue commutateur virtuel, cliquez sur **[Ajouter gestion réseau]** .
4. Sélectionnez **[VMkernel]** et cliquez sur **[Suivant]** .
5. Sélectionnez le vSwitch à utiliser ou sélectionnez **[Créer un commutateur virtuel]** pour créer un nouveau vSwitch.
6. Cochez les cases pour les adaptateurs réseau que vote vSwitch va utiliser.

   Sélectionnez les adaptateurs pour chaque vSwitch afin que les machines virtuelles ou les autres services se connectant via l'adaptateur puissent atteindre le segment Ethernet correspondant. Si aucun adaptateur n'apparaît dans Créer un nouveau commutateur virtuel, tous les adaptateurs réseau du système sont utilisés par les vSwitch existants. Vous pouvez créer un nouveau vSwitch sans adaptateur réseau ou sélection un adaptateur réseau utilisé par un vSwitch existant.
7. Cliquez sur **[Suivant]** .

8 Sélectionnez ou entrez une étiquette réseau ou un ID de VLAN.

Option	Description
[Étiquette de réseau]	Nom indentifiant le groupes de ports que vous créez. Il s'agit de l'étiquette que vous définissez lors de la configuration d'un adaptateur virtuel à associer à ce groupes de ports, lors de la configuration des services VMkernel, tels que vMotion et le stockage IP.
[ID VLAN]	Identifie le VLAN que le trafic réseau du groupes de ports utilisera.

9 Sélectionnez **[Utiliser ce groupes port pour vMotion]** pour permettre à ce groupes de ports de s'annoncer à un autre hôte comme connexion réseau où le trafic de vMotion doit être envoyé.

Vous pouvez activer cette propriété pour un seul groupes de ports vMotion et de stockage IP pour chaque hôte. Si cette propriété n'est pas activée pour un groupes de ports, la migration avec vMotion vers cet hôte n'est pas possible.

10 Choisissez d'utiliser ce groupe de ports pour l'enregistrement de la tolérance aux pannes.

11 Sur un hôte IPv6, indiquez si vous voulez utiliser **[IP (par défaut)]** , **[IPv6]** ou **[protocoles réseau IP et IPv6]** .

Cette option n'apparaît pas sur les hôtes sur lesquels IPv6 n'est pas activé. La configuration IPv6 ne peut pas être utilisée avec les adaptateurs iSCSI matériels dépendants.

12 Cliquez sur **[Suivant]** .

13 Sélectionnez **[Obtenir automatiquement les paramètres IP]** pour utiliser le DHCP pour obtenir les paramètres IP ou sélectionnez **[Utiliser les paramètres IP suivants]** pour définir les paramètres IP manuellement.

Si vous choisissez de définir les paramètres IP manuellement, fournissez ces informations.

DHCP ne peut pas être utilisée avec les adaptateurs iSCSI matériels dépendants.

a Entrez l'adresse IP et un masque de sous-réseau pour l'interface VMkernel.

Cette adresse doit être différente de l'adresse IP définie pour la console du service.

b Cliquez sur **[Modifier]** pour définir la passerelle par défaut de VMkernel pour les services de VMkernel, tels que vMotion, NAS et iSCSI.

c Dans l'onglet **[Config. DNS]** , le nom de l'hôte est entré par défaut.

Les adresses de serveur DNS spécifiées pendant l'installation sont également présélectionnées, de même que le domaine.

d Dans l'onglet **[Routage]** , la console du service et VMkernel ont chacun besoin de leurs propres informations de passerelle.

Une passerelle est nécessaire pour la connectivité aux machines qui ne sont pas sur le même sous-réseau IP que la console du service ou VMkernel. La valeur par défaut est le paramètre IP statique.

e Cliquez sur **[OK]** , puis sur **[Suivant]** .

14 Si vous utilisez IPv6 pour l'interface VMkernel, sélectionnez l'une des options suivantes pour obtenir les adresses IPv6.

- **[Obtenir adresse IPv6 automatiquement via DHCP]**
- **[Obtenir l'adresse IPv6 automatiquement via publicité routeur]**
- **[Adresses IPv6 statiques]**

15 Si vous choisissez d'utiliser des adresses IPv6 statiques, procédez comme suit.

   a Cliquez sur **[Ajouter]** pour ajouter une nouvelle adresse IPv6.

   b Entrez l'adresse IPv6 et la longueur du préfixe de sous-réseau, puis cliquez sur **[OK]** .

   c Pour modifier la passerelle par défaut de VMkernel, cliquez sur **[Modifier]** .

16 Cliquez sur **[Suivant]** .

17 Vérifiez les informations, cliquez sur **[Retour]** pour modifier des entrées, puis cliquez sur **[Terminer]** .

Configuration de la console du service

La console du service et VMkernel utilisent des adaptateurs Ethernet virtuels pour se connecter à un vSwitch et atteindre les réseaux que le vSwitch dessert.

Les modifications communes de la configuration de la console du service comprennent le changement des NIC et le changement des paramètres pour un NIC en cours d'utilisation.

S'il y a une seule connexion à la console du service, le changement de la configuration de cette dernière n'est pas autorisé. Pour une nouvelle connexion, changez les paramètres réseau pour utiliser un NIC supplémentaire. Après avoir vérifié que la nouvelle connexion fonctionne correctement, supprimez l'ancienne connexion. Vous passez sur le nouveau NIC.

Vous pouvez créer un maximum de 16 ports de console de service dans ESX.

Configuration du réseau de la console du service

Une seule interface réseau de la console du service est configurée au cours du processus d'installation ESX. Vous pouvez également ajouter des interfaces de console du service supplémentaires après l'installation et le démarrage d'ESX.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** , puis sur **[Mise en réseau]** .

3 Dans la vue commutateur virtuel, cliquez sur **[Ajouter gestion réseau]** .

4 Sélectionnez **[Console de service]** et cliquez sur **[Suivant]** .

5 Sélectionnez le vSwitch à utiliser pour l'accès au réseau, ou sélectionnez **[Créer un nouveau vSwitch]** , puis cliquez sur **[Suivant]** .

   Si aucun adaptateur n'apparaît dans créer un nouveau commutateur virtuel group, tous les adaptateurs réseau du système sont utilisés par les vSwitch existants.

6 Entrez l'étiquette réseau et l'ID de VLAN, et cliquez sur **[Suivant]** .

7 Entrez l'adresse IP et le masque de sous-réseau ou sélectionnez **[Obtenir automatiquement les paramètres IP]** .

8 Cliquez sur **[Modifier]** pour définir la passerelle par défaut de la console du service, puis cliquez sur **[Suivant]** .

9 Sur un hôte IPV6, sélectionnez **[Aucun paramètre IPv6]** pour utiliser les paramètres IPv4 uniquement pour la console du service, ou sélectionnez **[Utiliser les paramètres IPv6 suivants]** pour configurer IPv6 pour la console du service.

   Cet écran n'apparaît pas si IPv6 est désactivé sur l'hôte.

10 Si vous choisissez d'utiliser IPv6, sélectionnez comment obtenir les adresses IPv6.

11 Si vous choisissez **[Adresses IPv6 statiques]** , procédez comme suit :

   a Cliquez sur **[Ajouter]** pour ajouter une nouvelle adresse IPv6.

   b Entrez l'adresse IPv6 et la longueur du préfixe de sous-réseau, puis cliquez sur **[OK]** .

   c Pour modifier la passerelle par défaut de la console du service, cliquez sur **[Modifier]** .

12 Cliquez sur **[Suivant]** .

13 Vérifiez les informations, cliquez sur **[Retour]** pour modifier des entrées, puis cliquez sur **[Terminer]** .

Configuration des ports de la console du service

Vous pouvez modifier les propriétés des ports de la console du service, notamment les paramètres IP et les règles réseau.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** , puis sur **[Mise en réseau]** .

3 Sur le côté droit de la page, cliquez sur **[Propriétés]** pour le vSwitch que vous souhaitez modifier.

4 Dans la boîte de dialogue Propriétés de vSwitch, cliquez sur l'onglet **[Ports]** .

5 Sélectionnez **[Console de service]** et cliquez sur **[Modifier]** .

6 Pour continuer la configuration de la console du service, cliquez sur **[Continuer de modifier cette connexion]** .

7 Modifiez les propriétés de port, les paramètres IP et les règles effectives selon les besoins.

8 Cliquez sur **[OK]** .

Définition de la passerelle par défaut

Vous pouvez configurer une passerelle par défaut pour la console du service sur la pile TCP/IP. Le routage n'est pas disponible pour les configurations logicielles des chemins multiples iSCSI ni pour les adaptateurs iSCSI matériels dépendants.

AVERTISSEMENT Assurez-vous que vos paramètres réseau sont corrects avant d'enregistrer vos modifications. Si les paramètres réseau sont mal configurés, l'interface utilisateur peut perdre la connectivité à l'hôte, mais vous devez ensuite reconfigurer l'hôte à partir de la ligne de commande sur la console du service.

Procédure

1 Connectez-vous à vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** , puis sur **[DNS and Routing]** .

3 Cliquez sur **[Propriétés]** .

4 Cliquez sur l'onglet **[Routage]** .

5 Sous Console de service, définissez la passerelle par défaut et le périphérique de passerelle pour le réseau de la console du service.

Pour la console du service, le périphérique de passerelle est nécessaire seulement si plusieurs adaptateurs réseau utilisent le même sous-réseau. Le périphérique de passerelle détermine quel adaptateur réseau à utiliser pour l'acheminement par défaut.

La console du service et VMkernel ne sont souvent pas connectés au même réseau, chacun a besoin de ses propres informations de passerelle. Une passerelle est nécessaire pour la connectivité aux machines qui ne sont pas sur le même sous-réseau IP que la console du service ou les interfaces VMkernel.

Sur un hôte IPv6, vous pouvez également sélection une passerelle par défaut pour IPv6 et un périphérique de passerelle pour IPv6 pour le réseau de la console du service.

6 Spus VMkernel, définissez la passerelle par défaut pour le réseau VMkernel.

Sur un hôte IPv6, vous pouvez également sélection une passerelle par défaut pour IPv6 pour le réseau VMkernel.

7 Cliquez sur **[OK]** .

Affichage des informations de la console du service

Vous pouvez consulter les informations réseau de la console du service, notamment l'ID du VLAN et les règles réseau.

Procédure

1 Cliquez sur l'icône d'informations située à gauche du groupes de ports de la console du service pour afficher les informations de celle-ci.

2 Cliquez sur **[X]** pour fermer la fenêtre d'informations en incrustation.

Utilisation du DHCP pour la console du service

Dans la plupart des cas, vous utilisez les adresses IP pour la console du service. Vous pouvez également configurer la console du service pour utiliser l'adressage dynamique, DHCP, si votre serveur DNS peut mapper le nom d'hôte de la console du service sur l'adresse IP générée dynamiquement.

Si votre serveur DNS ne peut pas mapper le nom d'hôte sur son adresse générée par DHCP, utilisez l'adresse IP numérique de la console du service pour accéder à l'hôte. L'adresse IP numérique peut changer, lorsque le bail DHCP expire ou lorsque le système est redémarré. Pour cette raison, VMware ne recommande pas d'utiliser le DHCP pour la console du système à moins que votre serveur DNS puisse traiter la traduction du nom d'hôte.

Propriétés de commutateur standard vNetwork

Les paramètres de commutateur standard vNetwork contrôlent les valeurs par défaut des vSwitch pour les ports, qui peuvent être remplacées par les paramètres de groupes de ports pour chaque vSwitch. Vous pouvez éditer les propriétés des vSwitch, telles que la configuration de la liaison montante et le nombre de ports disponibles.

Modification du nombre de ports pour un vSwitch

Un commutateur virtuel sert de conteneur pour les configurations de ports qui utilisent un ensemble commun d'adaptateurs réseau, y compris les ensembles qui ne contiennent aucun adaptateur réseau. Chaque commutateur virtuel fournit un nombre déterminé de ports à travers lesquels les machines virtuelles et les services réseau peuvent atteindre un ou plusieurs réseaux.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Mise en réseau]** .

3 Sur le côté droit de la page, cliquez sur **[Propriétés]** pour le vSwitch que vous souhaitez modifier.

4 Cliquez sur l'onglet **[Ports]** .

5 Sélectionnez l'élément vSwitch dans la liste Configuration et cliquez sur **[Modifier]** .

6 Cliquez sur l'onglet **[Général]** .

7 Choisissez le nombre de ports que vous souhaitez utiliser dans le menu déroulant.

8 Cliquez sur **[OK]** .

Suivant

Les modifications entreront en vigueur au redémarrage du système.

Modification de la vitesse d'un adaptateur de liaison montante

Vous pouvez modifier la vitesse de connexion et le duplex d'un adaptateur de liaison montante.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Mise en réseau]** .

3 Sélectionnez un commutateur vSwitch et cliquez sur **[Propriétés]** .

4 Cliquez sur l'onglet **[Adaptateurs réseau]** .

5 Pour modifier la vitesse configurée et la valeur de duplex d'un adaptateur réseau, sélectionnez l'adaptateur réseau et cliquez sur **[Modifier]** .

6 Pour sélection la vitesse de connexion manuellement, sélectionnez la vitesse et le duplex dans le menu déroulant.

Choisissez la vitesse de connexion manuellement si la carte réseau et le commutateur physique risquent d'échouer dans la négociation de la vitesse de connexion correcte. Les symptômes de non-correspondance de vitesse et de duplex comprennent une bande passante faible ou aucune connectivité de liaison.

L'adaptateur et le port du commutateur physique auquel il est connecté doivent être définis sur la même valeur, telle que auto et auto ou ND et ND, où ND correspond à une certaine vitesse et à un duplex, mais pas à auto et ND.

7 Cliquez sur **[OK]** .

Ajout d'adaptateurs de liaison montante

Vous pouvez associer plusieurs adaptateurs à un seul vSwitch pour fournir l'association de cartes réseau. L'association peut partager du trafic et fournir un basculement.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Mise en réseau]** .

3 Sélectionnez un commutateur vSwitch et cliquez sur **[Propriétés]** .

4 Cliquez sur l'onglet **[Adaptateurs réseau]** .

5 Cliquez sur **[Ajouter]** pour lancer l'assistant Ajouter adaptateur.

6 Sélectionnez un ou plusieurs adaptateurs dans la liste et cliquez sur **[Suivant]** .

7 (Facultatif) Pour réorganiser les cartes réseau dans une catégorie différente, sélectionnez un adapteur et cliquez sur **[Monter]** et **[Descendre]** .

Option	Description
Adaptateurs actifs	Adaptateurs que le vSwitch utilise.
Adaptateurs de réserve	Adaptateurs qui deviennent actifs si un ou plusieurs adaptateurs actifs sont défaillants.

8 Cliquez sur **[Suivant]** .

9 Vérifiez les informations sur la page Résumé d'adaptateur, cliquez sur **[Retour]** pour modifier des entrées, puis cliquez sur **[Terminer]** .

La liste des adaptateurs réseau réapparaît, affichant les adaptateurs que le vSwitch demande maintenant.

10 Cliquez sur **[Fermer]** pour quitter la boîte de dialogue Propriétés vSwitch.

La section Mise en réseau de l'onglet **[Configuration]** montre les adaptateurs réseau dans l'ordre et les catégories désignés.

Protocole découverte Cisco

Protocole découverte Cisco(CDP) permet aux administrateurs ESX de déterminer quel port de commutateur Cisco est connecté à un vSwitch donné. Lorsque le CDP est activé pour un vSwitch particulier, vous pouvez afficher les propriétés du commutateur Cisco (telles que l'ID de périphérique, la version logicielle et le délai d'expiration) à partir de vSphere Client.

Activation du CDP sur un hôte ESX

Les vSwitch sont définis pour détecter les informations de port Cisco par défaut. Vous pouvez également définir le mode CDP afin qu'un vSwitch rende disponible des informations pour l'administrateur du commutateur Cisco.

Procédure

1 Connectez-vous directement à la console de votre hôte ESX.

2 Affichez le mode CDP en cours pour un vSwitch en entrant la commande **`esxcfg-vswitch -b <vSwitch>`**.

Si CDP est activé, le mode sera affiché comme **[Bas]** .

3 Modifiez le mode CDP en entrant la commande **`esxcfg-vswitch -B <mode> <vSwitch>`**.

Mode	Description
`down`	CDP est activé.
`listen`	ESX détecte et affiche les informations sur le port de commutateur Cisco associé, mais les informations sur le vSwitch ne sont pas disponibles pour l'administrateur du commutateur Cisco.
`advertise`	ESX rend disponible les informations sur le vSwitch pour l'administrateur du commutateur Cisco, mais ne détecte, ni n'affiche d'informations sur le commutateur Cisco.
`both`	ESX détecte et affiche les informations sur le commutateur Cisco associé et met les informations sur le vSwitch à la disposition de l'administrateur du commutateur Cisco.

Affichage des informations de commutateur Cisco sur vSphere Client

Lorsque CDP est défini sur **[Écouter]** ou **[Les deux]** , vous pouvez afficher les informations du commutateur Cisco.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Mise en réseau]** .

3 Cliquez sur l'icône d'informations à la droite du vSwitch.

Remarque Comme les annonces CDP de l'équipement Cisco surviennent généralement une fois toutes les minutes, un retard perceptible peut survenir entre l'activation CDP sur ESX et la disponibilité des données CDP à partir de vSphere Client.

Mise en réseau basique avec des commutateurs distribués vNetwork

4

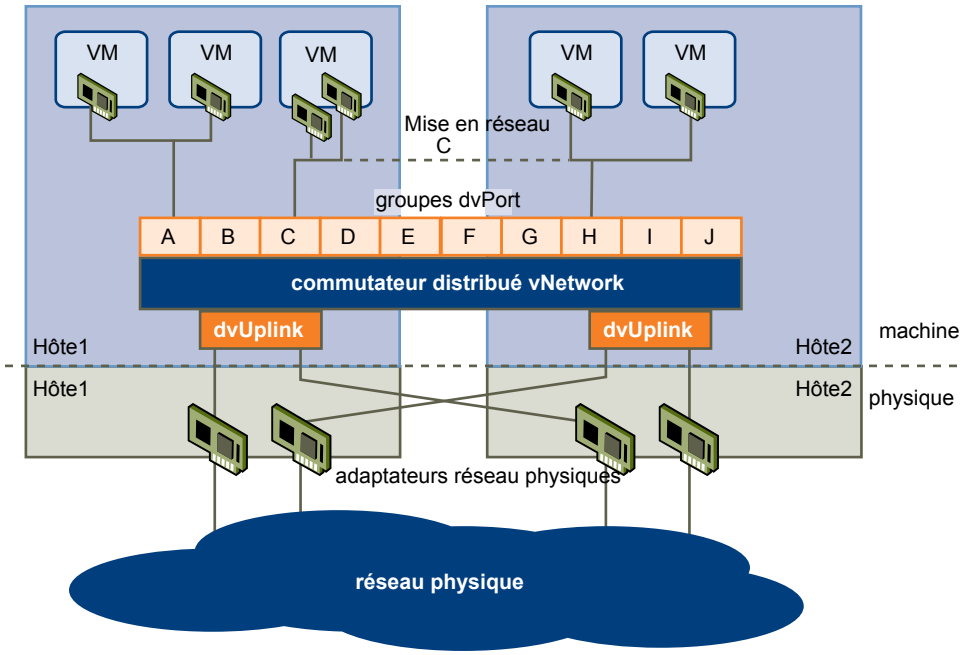
Ces sections vous guident à travers les concepts fondamentaux de mise en réseau avec des commutateurs distribués vNetwork et vous expliquent comment paramétrer et configurer la mise en réseau avec des commutateurs distribués vNetwork dans un environnement vSphere.

Ce chapitre aborde les rubriques suivantes :

Architecture de commutation distribuée vNetwork

Un commutateur distribué vNetwork (vDS) fonctionne en tant que commutateur virtuel unique sur tous les hôtes associés. Cela permet de régler les configurations réseau qui s'étendent sur tous les hôtes membres et permet aux machines virtuelles de conserver une configuration réseau cohérente lorsqu'elles migrent à travers plusieurs hôtes.

Figure 4-1. Réseau de commutateur distribué vNetwork



Comme un commutateur vNetwork standard, chaque commutateur distribué vNetwork est un concentrateur de réseau que les machines virtuelles peuvent utiliser. Un commutateur distribué vNetwork peut acheminer le trafic en interne entre les machines virtuelles, ou se lier à un réseau externe en se connectant à des cartes Ethernet physiques, également dénommées cartes de liaison montante.

Chaque commutateur distribué vNetwork peut également avoir un ou plusieurs groupes de dvPort qui lui sont affectés. Les groupes dvPort regroupesnt plusieurs ports sous une configuration commune et fournissent un point d'ancrage stable aux machines virtuelles qui se connectent aux réseaux étiquetés. Chaque groupes dvPort est identifié par une étiquette réseau, qui est unique au centre de données actuel. L'ID de VLAN est facultative. Elle permet de limiter le trafic du groupes de ports à un segment Ethernet logique dans le réseau physique.

Les pools de ressources réseau permettent de gérer le trafic réseau par type de trafic réseau.

En plus des commutateurs distribués vNetwork de VMware, vSphere 4 fournit également une assistance pour les commutateurs virtuels tiers. Pour plus d'informations sur la configuration des commutateurs tiers, rendez-vous à l'adresse http://www.cisco.com/go/1000vdocs.

Configurer un commutateur distribué vNetwork

Vous pouvez créer un commutateur distribué vNetwork sur un centre de données vCenter Server. Après avoir créé un commutateur distribué vNetwork, vous pouvez ajouter des hôtes, créer des groupes dvPort et modifier les règles et propriétés du commutateur distribué vNetwork.

Créer un commutateur distribué vNetwork

Créez un commutateur distribué vNetwork afin de gérer le trafic de mise en réseau pour les hôtes associés sur le centre de données.

Procédure

1 Ouvrez une session sur le vSphere Client et choisissez la vue d'inventaire Mise en réseau.

2 Dans le menu Inventaire, sélectionnez **[Centre de données] > [Commutateur distribué vNetwork]** .

3 Choisissez une version de commutateur distribué vNetwork.

Option	Description
Version de commutateur distribué vNetwork : 4.0	Compatible avec la version ESX 4.0 et ultérieure. Les fonctions publiées avec les versions ultérieures de vDS ne sont pas prises en charge.
Version de commutateur distribué vNetwork : 4.1.0	Compatible avec la version ESX 4.1 ou ultérieure.

4 Cliquez sur **[Suivant]** .

5 Saisissez un nom pour le commutateur distribué vNetwork dans la zone de texte Name Nom.

6 Utilisez les boutons fléchés pour sélectionner le **[Nombre de ports dvUplink]** et cliquez sur **[Suivant]** .

Les ports dvUplink connectent un commutateur distribué vNetwork aux adaptateurs réseau physiques sur les hôtes associés. Le nombre de ports dvUplink est le nombre maximum de connections physiques autorisées vers le commutateur distribué vNetwork par hôte.

7 Choisissez le moment pour ajouter des hôtes au vDS.

Option	Description
Ajouter maintenant	Sélectionnez les hôtes et les cartes physiques à utiliser en cochant la case correspondant à chaque hôte ou carte. Vous pouvez uniquement ajouter les cartes physiques qui ne sont pas déjà utilisées dans la création du commutateur distribué vNetwork.
Ajouter plus tard	Aucun hôte ajouté au vDS pour l'instant. Vous devez ajouter des hôtes au vDS avant d'ajouter des cartes réseau. Vous pouvez ajouter des cartes réseau depuis la page de configuration d'hôte de vSphere Client en utilisant la fonctionnalité de gestion des hôtes ou Profils d'hôte.

8 Cliquez sur **[Suivant]** .

9 (Facultatif) Choisissez **[Créer automatiquement groupe ports par défaut]** .

Cette option crée un groupes de ports à liaison statique avec des ports 128. Pour les systèmes dont les conditions requises sur les groupes de ports sont complexes, ignorez le groupes de ports par défaut et créez un nouveau groupes dvPort après avoir terminé d'ajouter le commutateur distribué vNetwork.

10 Passez en revue le diagramme du commutateur distribué vNetwork pour garantir une configuration adéquate, puis cliquez sur **[Terminer]** .

Ajouter des hôtes à un commutateur distribué vNetwork

Vous pouvez ajouter des hôtes et des cartes physiques à un commutateur distribué vNetwork au niveau vDS après la création du vDS.

Procédure

1 Dans vSphere Client, affichez la vue d'inventaire de réseau et sélectionnez le commutateur distribué vNetwork.

2 Sélectionnez **[Inventaire] > [commutateur distribué vNetwork] > [Ajout hôte]** .

3 Sélectionnez les hôtes à ajouter.

4 Sous les hôtes sélectionnés, sélectionnez les cartes physiques à ajouter et cliquez sur **[Suivant]** .

Vous pouvez sélection des adaptateurs physiques libres et en cours d'utilisation.

REMARQUE Le déplacement d'un adaptateur physique vers un vDS sans les adaptateurs virtuels associés peut entraîner la perte de connexion réseau à ces adaptateurs virtuels.

---

5 Pour chaque carte virtuelle, sélectionnez **[groupes ports destination]** dans le menu déroulant pour faire migrer la carte virtuelle vers le vDS ou sélectionnez **[Ne pas migrer]** .

6 Cliquez sur **[Suivant]** .

7 (Facultatif) Faites migrer la gestion de réseau des machines virtuelles vers le vDS.

a Sélectionnez **[Migrer mise en réseau VM]** .

b Pour chaque machine virtuelle, sélectionnez le groupes de ports de destination **[groupes ports destination]** dans le menu déroulant ou sélectionnez **[Ne pas migrer]** .

8 Cliquez sur **[Suivant]** .

9 Passez en revue les paramètres du vDS et cliquez sur **[Terminer]** .

Si vous devez apporter des modifications, cliquez sur **[Retour]** pour revenir à l'écran approprié.

Gérer les hôtes sur un vDS

Vous pouvez modifier la configuration des hôtes et des adaptateurs physiques sur un vDS après leur ajout au vDS.

Procédure

1 Dans vSphere Client, affichez la vue d'inventaire de réseau et sélectionnez le commutateur distribué vNetwork.

2 Sélectionnez **[inventaire] > [commutateur distribué vNetwork] > [Gérer les hôtes]** .

3 Sélectionnez les hôtes à gérer et cliquez sur **[Suivant]** .

4 Sélectionnez les adaptateurs physiques à ajouter, désélectionnez les adaptateurs physiques à supprimer, et cliquez sur **[Suivant]** .

5 Pour chaque carte virtuelle, sélectionnez **[groupes ports destination]** dans le menu déroulant pour faire migrer la carte virtuelle vers le vDS ou sélectionnez **[Ne pas migrer]** .

6 Cliquez sur **[Suivant]** .

7 (Facultatif) Faites migrer la gestion de réseau des machines virtuelles vers le vDS.

   a Sélectionnez **[Migrer mise en réseau VM]** .

   b Pour chaque machine virtuelle, sélectionnez le groupes de ports de destination **[groupes ports destination]** dans le menu déroulant ou sélectionnez **[Ne pas migrer]** .

8 Cliquez sur **[Suivant]** .

9 Passez en revue les paramètres du vDS et cliquez sur **[Terminer]** .

   Si vous devez apporter des modifications, cliquez sur **[Retour]** pour revenir à l'écran approprié.

Modifier les paramètres généraux de commutateur distribué vNetwork

Vous pouvez modifier les propriétés générales du commutateur distribué vNetwork, comme par exemple le nom du commutateur distribué vNetwork et le nombre de ports de liaison montante sur le commutateur distribué vNetwork.

Procédure

1 Dans vSphere Client, choisissez la vue d'inventaire de mise en réseau et sélectionnez le commutateur distribué vNetwork.

2 Dans le menu Inventaire, sélectionnez **[Commutateur distribué vNetwork]** > **[Modifier les paramètres]** .

3 Sélectionnez **[Général]** pour modifier les paramètres de commutateur distribué vNetwork suivants.

   - Écrivez le nom du commutateur distribué vNetwork.
   - Sélectionnez le nombre de ports de liaison montante.
   - Pour modifier des noms de port de liaison montante, cliquez sur **[Modifier les noms des ports pour liaisons montantes]** , entrez les nouveaux noms, puis cliquez sur **[OK]** .
   - Entrez des remarques éventuelles sur le commutateur distribué vNetwork.

4 Cliquez sur **[OK]** .

Modifier les paramètres avancés de commutateur distribué vNetwork

Utilisez la boîte de dialogue de paramètres de commutateur distribué vNetwork pour configurer les paramètres avancés de commutateur distribué vNetwork tels que le protocole de découverte Cisco et la MTU maximum.

Procédure

1 Dans vSphere Client, affichez la vue d'inventaire de mise en réseau et sélectionnez le commutateur distribué vNetwork.

2 Dans le menu Inventaire, sélectionnez **[commutateur distribué vNetwork]** > **[Modifier les paramètres]** .

3 Sélectionnez **[Avancé]** pour modifier les propriétés suivantes de commutateur distribué vNetwork.

   a Indiquez la taille de MTU maximum.

   b Cochez la case **[Activer Protocole découverte Cisco]** pour activer le protocole CDP, et réglez l'opération sur **[Écouter]** , **[Annoncer]** ou **[Les deux]** .

   c Tapez le nom et autres renseignements sur l'administrateur de commutateur distribué vNetwork dans la section Informations de contact admin.

4 Cliquez sur **[OK]** .

Afficher les informations de l'adaptateur réseau pour un commutateur vNetwork distribué

Affichez les adaptateurs réseau physiques et les attributions de liaison montante pour un commutateur distribué vNetwork depuis la vue d'inventaire de mise en réseau du vSphere Client.

Procédure

1 Dans vSphere Client, choisissez la vue d'inventaire de mise en réseau et sélectionnez le commutateur distribué vNetwork.

2 Dans le menu Inventaire, sélectionnez **[commutateur distribué vNetwork] > [Modifier les paramètres]** .

3 Dans l'onglet **[Adaptateurs réseau]** , vous pouvez afficher la carte réseau et les attributions de liaison montante des hôtes associés.

Cet onglet est en lecture seule. Les cartes réseau du commutateur distribué vNetwork doivent être configurées au niveau de l'hôte.

4 Cliquez sur **[OK]** .

Mettre à niveau un vDS vers une version plus récente

Un commutateur distribué vNetwork de version 4.0 peut bénéficier d'une mise à niveau vers la version 4.1, lui permettant de tirer profit des fonctions disponibles uniquement dans la version ultérieure.

Procédure

1 Dans vSphere Client, affichez la vue d'inventaire de réseau et sélectionnez le commutateur distribué vNetwork.

2 Dans l'onglet **[Résumé]** , en regard de **[Version]** , sélectionnez **[Mise à niveau]** .

L'assistant de mise à niveau répertorie les fonctions disponibles pour le vDS mis à niveau et inaccessibles à la version précédente.

3 Cliquez sur **[Suivant]** .

L'assistant de mise à niveau répertorie les hôtes associés à ce vDS et leur compatibilité avec la version vDS mise à niveau. Vous ne pouvez poursuivre la mise à niveau que si tous les hôtes sont compatibles avec la nouvelle version vDS.

À côté de chaque hôte incompatible, l'assistant de mise à niveau répertorie les raisons de l'incompatibilité.

4 Cliquez sur **[Suivant]** .

5 Vérifiez l'exactitude des informations de mise à niveau répertoriées et cliquez sur **[Terminer]** .

groupes dvPort

Un groupes dvPort spécifie les options de configuration de port pour chaque port membre sur un commutateur distribué vNetwork. Les groupes dvPort définissent la manière dont s'établit une connexion à un réseau.

Ajoutez un groupes dvPort

Utilisez l'assistant Créer un groupe dvPort pour ajouter un groupes dvPort à un commutateur distribué vNetwork.

Procédure

1 Dans vSphere Client, affichez la vue d'inventaire de mise en réseau et sélectionnez le commutateur distribué vNetwork.

2 À partir du menu **[inventaire]** , sélectionnez **[Commutateur virtuel distribué] > [Nouveau groupes de ports]** .

3 Entrez un nom et le nombre de ports pour le groupes dvPort.

4 Sélectionnez un type de VLAN.

Option	Description
Aucune	N'utilise pas de VLAN.
VLAN	Dans le champ **[ID VLAN]** , entrez un nombre entre 1 et 4094.
jonction VLAN	Entrez une plage de jonctions VLAN.
VLAN privé	Sélectionnez une entrée de VLAN privé. Si vous n'avez créé aucun VLAN privé, ce menu est vide.

5 Cliquez sur **[Suivant]** .

6 Cliquez sur **[Terminer]** .

Modifier les propriétés générales de groupes dvPort

Utilisez la boîte de dialogue dvPort Group Properties pour configurer les propriétés générales de groupes dvPort, telles que le nom de groupes dvPort et le type de groupes de port.

Procédure

1 Dans vSphere Client, affichez la vue d'inventaire Mise en réseau et sélectionnez le groupes dvPort.

2 Dans le menu Inventaire, sélectionnez **[Réseau] > [Modifier les paramètres]** .

3 Sélectionnez **[Général]** pour modifier les propriétés de groupes dvPort suivantes.

Option	Action
Nom	Entrez le nom du groupes dvPort.
Description	Entrez une brève description du groupes dvPort.

Option	Action
Nombre de ports	Entrez le nombre de ports sur le groupes dvPort.
Liaison de port	Choisissez quand les ports sont affectés aux machines virtuelles connectées à ce groupes dvPort. ■ Sélectionnez **[Liaison statique]** pour affecter un port à une machine virtuelle quand la machine virtuelle est connectée au groupes dvPort. ■ Sélectionnez **[Liaison dynamique]** pour affecter un port à une machine virtuelle à la première mise sous tension de la machine virtuelle une fois connectée au groupes dvPort. ■ Sélectionnez **[Éphémère]** pour aucune liaison de port. Vous pouvez choisir une liaison éphémère uniquement lorsque vous êtes connecté directement à votre hôte ESX.

4 Cliquez sur **[OK]** .

Modifier les propriétés avancées de groupes dvPort

Utilisez la boîte de dialogue Propriétés de groupes dvPort pour configurer les propriétés avancées de groupes dvPort, telles que les paramètres de remplacement de port.

Procédure

1 Dans vSphere Client, affichez la vue d'inventaire Mise en réseau et sélectionnez le groupes dvPort.

2 Dans le menu Inventaire, sélectionnez **[Réseau] > [Modifier les paramètres]** .

3 Sélectionnez **[Avancé]** pour modifier les propriétés de groupes dvPort.

   a Sélectionnez **[Autoriser remplacement règles port]** pour autoriser le remplacement des règles de groupes dvPort au niveau du port.

   b Cliquez sur **[Modifier paramètres remplacement]** pour sélection les règles qui peuvent être remplacées.

   c Choisissez d'autoriser le déplacement de ports actifs.

   d Sélectionnez **[Configurer réinitialisation à la déconnexion]** pour ignorer les configurations par port lorsqu'un dvPort est déconnecté d'une machine virtuelle.

4 Cliquez sur **[OK]** .

dvPorts

Un dvPort est un port sur un commutateur distribué vNetwork qui se connecte à la console de service, au VMkernel d'un hôte ou à la carte réseau d'une machine virtuelle.

Par défaut, la configuration d'un dvPort est déterminée par les paramètres de groupes de dvPorts, mais certains paramètres pour des dvPorts individuels peuvent être ignorés selon le dvPort.

Surveiller l'état du dvPort

vSphere peut surveiller les dvPort et fournir des informations sur leur état actuel respectif.

Procédure

1 Dans vSphere Client, affichez la vue d'inventaire de mise en réseau et sélectionnez le commutateur distribué vNetwork.

2 Dans l'onglet **[Ports]** , cliquez sur **[Commencer à surveiller l'état du port]** .

La colonne **[État]** dans l'onglet **[Ports]** pour le commutateur distribué vNetwork affiche désormais l'état actuel pour chaque dvPort.

Tableau 4-1. États de dvPort

État	Description
[Raccorder]	Le lien pour ce dvPort est actif.
[Lien bas]	Le lien pour ce dvPort est inactif.
[Bloqué]	Ce dvPort est bloqué.
[--]	L'état de ce dvPort est actuellement indisponible.

Configurer les paramètres dvPort

Utilisez la boîte de dialogue Paramètres de port pour configurer les propriétés générales de dvPort, telles que le nom de port et sa description.

Procédure

1 Ouvrez une session sur vSphere Client et affichez le commutateur distribué vNetwork.

2 Dans l'onglet **[Ports]** , cliquez avec le bouton droit sur le port à modifier et sélectionnez **[Modifier les paramètres]** .

3 Cliquez sur **[Général]** .

4 Modifiez la description et le nom du port.

5 Cliquez sur **[OK]** .

VLAN privés

Les VLAN privés servent à résoudre les restrictions d'ID VLAN et le gaspillage d'adresses IP pour certaines configurations réseau.

Un VLAN privé est identifié par son ID VLAN primaire. un ID VLAN primaire peut avoir plusieurs ID VLAN associées. Les VLAN primaires sont **[Promiscuité]** , afin que les ports sur un VLAN privé puissent communiquer avec des ports configurés en tant que VLAN primaire. Des ports sur un VLAN secondaire peuvent être **[Isolé]** et communiquer uniquement avec des ports de promiscuité, ou **[Communauté]** et communiquer avec des ports de promiscuité et d'autres ports sur le même VLAN secondaire.

Pour utiliser des VLAN privés entre un hôte ESX et le reste du réseau physique, le commutateur physique connecté à l'hôte ESX doit prendre en charge un VLAN privé et être configuré avec les ID VLAN utilisées par ESX pour la fonctionnalité du VLAN privé. Pour les commutateurs physiques utilisant un apprentissage par ID VLAN+MAC dynamique, toutes les ID VLAN privé correspondantes doivent être d'abord entrées dans la base de données VLAN du commutateur.

Afin de configurer des dvPorts pour utiliser la fonctionnalité VLAN privé, vous devez créer les VLAN privés requis sur le commutateur distribué vNetwork auquel les dvPorts sont connectés.

Créer un VLAN privé

Vous pouvez créer un VLAN privé à utiliser sur un commutateur distribué vNetwork ainsi que ses dvPorts correspondants.

Procédure

1 Dans vSphere Client, affichez la vue d'inventaire de mise en réseau et sélectionnez le commutateur distribué vNetwork.

2 Dans le menu **[Inventaire]** , sélectionnez **[commutateur distribué vNetwork] > [Modifier les paramètres]** .

3 Sélectionnez l'onglet **[VLAN privé]** .

4 Sous l'ID VLAN privé primaire, cliquez sur **[] [[Saisir un ID VLAN privé ici]]** , et saisissez le numéro de VLAN privé primaire.

5 Cliquez n'importe où dans la boîte de dialogue, puis sélectionnez le VLAN privé primaire que vous venez d'ajouter.

Ce dernier apparaît sous ID VLAN privé secondaire.

6 Pour chaque nouveau VLAN privé secondaire, cliquez sur **[[Saisir un ID VLAN privé ici]]** sous ID VLAN privé secondaire, et saisissez le numéro du VLAN privé secondaire.

7 Cliquez n'importe où dans la boîte de dialogue, sélectionnez le VLAN privé secondaire que vous venez d'ajouter, et sélectionnez **[Isolé]** ou **[Communauté]** comme type de port.

8 Cliquez sur **[OK]** .

Supprimer un VLAN privé principal

Supprimez les VLAN privés primaires non utilisés dans la vue d'inventaire de mise en réseau du vSphere Client.

Prérequis

Avant de supprimer un VLAN privé, assurez-vous qu'aucun groupes de port ne soit configuré pour l'utiliser.

Procédure

1 Dans vSphere Client, affichez la vue d'inventaire de mise en réseau et sélectionnez le commutateur distribué vNetwork.

2 Dans le menu **[Inventaire]** , sélectionnez **[commutateur distribué vNetwork] > [Modifier les paramètres]** .

3 Sélectionnez l'onglet **[VLAN privé]** .

4 Sélectionnez le VLAN privé principal à supprimer.

5 Cliquez sur **[Supprimer]** sous ID VLAN privé primaire, puis cliquez sur **[OK]** .

Le retrait d'un VLAN privé primaire supprime également l'ensemble des VLAN privés secondaires associés.

Supprimer un VLAN privé secondaire

Supprimez les VLAN privés secondaires non utilisés dans la vue d'inventaire de mise en réseau du vSphere Client.

Prérequis

Avant de supprimer un VLAN privé, assurez-vous qu'aucun groupes de port ne soit configuré pour l'utiliser.

Procédure

1 Dans vSphere Client, affichez la vue d'inventaire de mise en réseau et sélectionnez le commutateur distribué vNetwork.

2 Dans le menu **[Inventaire]** , sélectionnez **[commutateur distribué vNetwork] > [Modifier les paramètres]** .

3 Sélectionnez l'onglet **[VLAN privé]** .

4 Sélectionnez un VLAN privé principal pour afficher l'ensemble de ses VLAN privés secondaires associés.

5 Sélectionnez le VLAN privé secondaire à supprimer.

6 Cliquez sur **[Supprimer]** sous ID VLAN privé secondaire, puis cliquez sur **[OK]** .

Configurer des cartes réseau de commutateur distribué vNetwork

La vue du commutateur distribué vNetwork de la page de configuration de l'hôte affiche la configuration des commutateurs distribués vNetwork correspondants de l'hôte et permet de configurer les ports de liaison montante et les cartes réseau de commutateur distribué vNetwork.

Gestion des cartes physiques

Pour chaque hôte associé à un commutateur distribué vNetwork, vous devez affecter des adaptateurs réseau physiques, ou liaisons montantes, au commutateur distribué vNetwork. Vous pouvez affecter une liaison montante sur chaque hôte par port de liaison montante sur le commutateur distribué vNetwork.

Ajouter une liaison montante à un commutateur distribué vNetwork

Pour chaque hôte associé à un commutateur distribué vNetwork, vous devez affecter au moins un adapteur réseau physique, ou liaison montante, au commutateur distribué vNetwork.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez un hôte dans le panneau d'inventaire.

La page de configuration matérielle pour l'hôte sélectionné s'affiche.

2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Mise en réseau]** .

3 Choisir la vue **[Commutateur distribuée vNetwork]** .

4 Cliquez sur **[Gérer adaptateurs physiques]** .

5 Cliquez sur **[Cliquez pour ajouter carte réseau]** pour le port de liaison montante auquel ajouter une liaison montante.

6 Sélectionnez la carte physique à ajouter.

Si vous choisissez un adapteur attachée à un autre commutateur, elle est retirée de ce commutateur et réaffectée à ce commutateur distribué vNetwork.

7 Cliquez sur **[OK]** .

Supprimer une Liaison Montante d'un commutateur distribué vNetwork

Vous pouvez supprimer une liaison montante, ou l'adaptateur de réseau physique, d'un commutateur distribué vNetwork.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.

La page de configuration matérielle pour ce serveur s'affiche.

2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Mise en réseau]** .

3 Choisir la vue **[commutateur distribué vNetwork]** .

4 Cliquez sur **[Gérer adaptateurs physiques]** .

5 Cliquez sur **[Supprimer]** pour supprimer la liaison montante de **[commutateur distribué vNetwork]** .

6 Cliquez sur **[OK]** .

Gestion des cartes réseau virtuelles

Les cartes réseau virtuelles gèrent les services réseau de l'hôte sur un commutateur distribué vNetwork.

Vous pouvez configurer la console de service et les adaptateurs virtuels VMkernel pour un hôte ESX à travers un commutateur distribué vNetwork associé en créant de nouvelles cartes virtuelles ou en migrant des cartes virtuelles existantes.

Créer un adapteur réseau VMkernel sur un commutateur distribué vNetwork

Créez un adapteur réseau VMkernel utilisable en tant qu'interface vMotion ou que groupes de ports de stockage d'IP.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Mise en réseau]** .

3 Choisissez la vue de commutateur distribuée vNetwork.

4 Cliquez sur **[Gérer adaptateurs virtuels]** .

5 Cliquez sur **[Ajouter]** .

6 Sélectionnez **[Nouvel adaptateur virtuel]** et cliquez sur **[Suivant]** .

7 Sélectionnez **[VMkernel]** et cliquez sur **[Suivant]** .

8 Choisissez une connexion dvPort ou de groupe dvPort pour l'adaptateur virtuel.

Option	Description
Sélectionnez un groupe de ports	Choisissez le groupe dvPort auquel connecter l'adaptateur virtuel dans le menu déroulant.
Sélectionnez le port	Choisissez le dvPort auquel connecter l'adaptateur virtuel dans le menu déroulant.

9 Sélectionnez **[Utiliser cet adaptateur virtuel pour vMotion]** pour permettre à ce groupes de ports de s'annoncer à un autre hôte ESX comme connexion réseau où le trafic de vMotion est envoyé.

Vous pouvez activer cette propriété pour un seul groupes de ports vMotion et de stockage IP pour chaque hôte ESX. Si cette propriété n'est pas activée pour un groupes de ports, la migration avec vMotion vers cet hôte n'est pas possible.

10 Choisissez **[Utiliser cet adaptateur virtuel pour enregistrement tolérance pannes]** .

11 Sous les paramètres IP, précisez l'adresse IP et le masque de sous-réseau.

IPv6 ne peut pas être utilisée avec un adaptateur iSCSI matériel dépendant.

12 Cliquez sur **[Modifier]** pour définir la passerelle par défaut de VMkernel pour les services de VMkernel, tels que vMotion, NAS et iSCSI.

13 Dans l'onglet **[Config. DNS]** , le nom de l'hôte est entré par défaut. Le domaine et les adresses de serveur DNS spécifiées pendant l'installation sont également présélectionnés.

14 Dans l'onglet **[Routage]** , la console du service et VMkernel ont chacun besoin de leurs propres informations de passerelle. Une passerelle est nécessaire pour la connectivité aux machines qui ne sont pas sur le même sous-réseau IP que la console du service ou VMkernel.

Les paramètres IP sont statiques par défaut. N'utilisez pas le routage pour les configurations logicielles des chemins multiples iSCSI ni pour les adaptateurs iSCSI matériels dépendants.

15 Cliquez sur **[OK]** , puis sur **[Suivant]** .

16 Cliquez sur **[Terminer]** .

Créer un adapteur réseau de console de service sur un commutateur distribué vNetwork

Créer un adapteur réseau de console de service sur un commutateur distribué vNetwork pour supporter une mise en réseau de console de service d'hôte sur un vDS.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Mise en réseau]** .

3 Choisissez la vue de commutateur distribuée vNetwork.

4 Cliquez sur **[Gérer adaptateurs virtuels]** .

5 Cliquez sur **[Ajouter]** .

6 Sélectionnez **[Nouvel adaptateur virtuel]** et cliquez sur **[Suivant]** .

7 Sélectionnez **[Console de service]** et cliquez sur **[Suivant]** .

8 Choisissez une connexion dvPort ou de groupe dvPort pour l'adaptateur virtuel.

Option	Description
Sélectionnez un groupe de ports	Choisissez le groupe dvPort auquel connecter l'adaptateur virtuel dans le menu déroulant.
Sélectionnez le port	Choisissez le dvPort auquel connecter l'adaptateur virtuel dans le menu déroulant.

9 Saisissez l'adresse IP et le masque de sous-réseau ou sélectionnez **[Obtenir automatiquement les paramètres IP]** .

10 (Facultatif) Cliquez sur **[Modifier]** pour définir la passerelle par défaut de la console de service.

11 Cliquez sur **[Suivant]** .

12 Cliquez sur **[Terminer]** .

Migrer un adapteur virtuelle existante vers un commutateur distribué vNetwork

Vous pouvez migrer une carte virtuelle existante d'un commutateur standard vNetwork vers un commutateur distribué vNetwork.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Mise en réseau]** .

3 Choisissez la vue de commutateur distribuée vNetwork.

4 Cliquez sur **[Gérer adaptateurs virtuels]** .

5 Cliquez sur **[Ajouter]** .

6 Sélectionnez **[Migrer adaptateurs virtuels existants]** et cliquez sur **[Suivant]** .

7 Sélectionnez un ou plusieurs adaptateur de réseau virtuel à migrer.

8 Pour chaque carte sélectionnée, choisissez un groupes de ports dans le menu déroulant **[Choisir un groupe de ports]** .

9 Cliquez sur **[Suivant]** .

10 Cliquez sur **[Terminer]** .

Migrer un adaptateur virtuel à un commutateur standard vNetwork

Utilisez l'assistant Migrer vers commutateur virtuel pour migrer un adaptateur virtuel existant d'un commutateur distribué vNetwork sur un commutateur standard vNetwork.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.

La page de configuration matérielle pour ce serveur s'affiche.

2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Mise en réseau]** .

3 Choisir la vue **[commutateur distribué vNetwork]** .

4 Cliquez sur **[Gérer adaptateurs virtuels]** .

5 Sélectionnez l'adaptateur virtuel à migrer, et cliquez sur **[Migrer vers commutateur virtuel]** .

L'assistant Migrer l'adaptateur virtuel s'affiche.

6 Sélectionnez le vSwitch sur lequel migrer l'adaptateur et cliquez sur **[Suivant]** .

7 Entrez une **[Étiquette réseau]** et optionnellement un **[ID VLAN]** pour l'adaptateur virtuel et cliquez sur **[Suivant]** .

8 Cliquez sur **[Terminer]** pour migrer l'adaptateur virtuel et pour terminer l'assistant.

Modifier la configuration de VMkernel sur un commutateur distribué vNetwork

Vous pouvez modifier les propriétés d'un adapteur VMkernel existante sur un commutateur distribué vNetwork depuis l'hôte correspondant.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Mise en réseau]** .

3 Choisissez la vue de commutateur distribuée vNetwork.

4 Cliquez sur **[Gérer adaptateurs virtuels]** .

5 Sélectionnez l'adaptateur VMkernel à modifier et cliquez sur **[Modifier]** .

6 Choisissez une connexion dvPort ou de groupe dvPort pour l'adaptateur virtuel.

Option	Description
Sélectionnez un groupe de ports	Choisissez le groupe dvPort auquel connecter l'adaptateur virtuel dans le menu déroulant.
Sélectionnez le port	Choisissez le dvPort auquel connecter l'adaptateur virtuel dans le menu déroulant.

7 Sélectionnez **[Utiliser cet adaptateur virtuel pour vMotion]** pour permettre à ce groupes de ports de s'annoncer à un autre hôte ESX comme connexion réseau où le trafic de vMotion est envoyé.

Vous pouvez activer cette propriété pour un seul groupes de ports vMotion et de stockage IP pour chaque hôte ESX. Si cette propriété n'est pas activée pour un groupes de ports, la migration avec vMotion vers cet hôte n'est pas possible.

8 Choisissez **[Utiliser cet adaptateur virtuel pour enregistrement tolérance pannes]** .

9 Sous les paramètres IP, spécifiez l'adresse IP et le masque de sous-réseau, ou sélectionnez **[Obtenir les paramètres IP automatiquement]** .

10 Cliquez sur **[Modifier]** pour définir la passerelle par défaut de VMkernel pour les services de VMkernel, tels que vMotion, NAS et iSCSI.

11 Cliquez sur **[OK]** .

Modifier la configuration de la console de service sur un commutateur distribué vNetwork

Vous pouvez modifier les paramètres de port et d'IP pour un adaptateur de console de service existant sur un commutateur distribué vNetwork.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Mise en réseau]** .

3 Choisissez la vue de commutateur distribuée vNetwork.

4 Cliquez sur **[Gérer adaptateurs virtuels]** .

5 Sélectionnez l'adaptateur de console du service à modifier et cliquez sur **[Modifier]** .

6 Choisissez une connexion dvPort ou de groupe dvPort pour l'adaptateur virtuel.

Option	Description
Sélectionnez un groupe de ports	Choisissez le groupe dvPort auquel connecter l'adaptateur virtuel dans le menu déroulant.
Sélectionnez le port	Choisissez le dvPort auquel connecter l'adaptateur virtuel dans le menu déroulant.

7 Saisissez l'adresse IP et le masque de sous-réseau ou sélectionnez **[Obtenir automatiquement les paramètres IP]** .

8 (Facultatif) Cliquez sur **[Modifier]** pour définir la passerelle par défaut de la console de service.

9 Cliquez sur **[OK]** .

Supprimer un Adaptateur Virtuel

Retirez un adaptateur de réseau virtuel d'un commutateur distribué vNetwork dans la boîte de dialogue Gérer Adaptateurs Virtuels.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Mise en réseau]** .

3 Choisir la vue **[commutateur distribué vNetwork]** .

4 Cliquez sur **[Gérer adaptateurs virtuels]** .

5 Sélectionnez l'adaptateur virtuel à supprimer et cliquez sur **[Supprimer]** .

Une boîte de dialogue s'affiche avec le message,`Voulez-vous vraiment supprimer <adapter name> ?`

6 Cliquez sur **[Oui]** .

Configurer la mise en réseau de machines virtuelles sur un commutateur distribué vNetwork

Connectez les machines virtuelles à un commutateur distribué vNetwork en configurant un adaptateur d'interface réseau de machine virtuelle individuelle ou en migrant des groupes de travail de machines virtuelles depuis le commutateur distribué vNetwork.

Connectez les machines virtuelles aux commutateurs distribués vNetwork en connectant leurs cartes réseau virtuelles correspondantes aux groupes de travail dvPort. Vous pouvez le faire pour une machine virtuelle individuelle en modifiant la configuration de sa carte réseau, ou pour un groupes de machines virtuelles en migrant les machines virtuelles depuis un réseau virtuel existant vers un commutateur distribué vNetwork.

Migrer les machines virtuelles depuis ou vers un commutateur distribué vNetwork

En plus de la connexion de machines virtuelles à un commutateur distribué vNetwork (vDS) au niveau individuel, vous pouvez migrer un groupes de machines virtuelles entre un réseau vDS et un réseau de commutateur standard vNetwork.

Procédure

1 Dans vSphere Client, affichez la vue d'inventaire de mise en réseau et sélectionnez le commutateur distribué vNetwork.

2 Dans le menu **[inventaire]** , sélectionnez **[commutateur distribué vNetwork] > [Migrer la gestion de réseau de machines virtuelles]** .

L'assistant Migrer la mise en réseau de machines virtuelles apparaît.

3 Dans le menu déroulant **[Choisir le réseau source]** , sélectionnez le réseau virtuel source de la migration.

4 Sélectionnez le réseau virtuel cible de la migration dans le menu déroulant **[Choisir le réseau de destination]** .

5 Cliquez sur **[Afficher machines virtuelles]** .

Les machines virtuelles associées au réseau virtuel à l'origine de la migration s'affichent dans le champ **[Sélectionner machines virtuelles]** .

6 Sélectionnez les machines virtuelles à migrer vers le réseau virtuel de destination et cliquez sur **[OK]** .

Connecter une machine virtuelle individuelle à un groupes dvPort

Connectez une machine virtuelle individuelle à un commutateur distribué vNetwork en modifiant la configuration de la carte d'interface réseau de la machine virtuelle.

Procédure

1 Ouvrez une session sur le vSphere Client et sélectionnez la machine virtuelle dans le panneau d'inventaire.

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

3 Dans l'onglet **[Matériel]** , sélectionnez la carte réseau virtuelle.

4 Sélectionnez le groupes dvPort vers lequel migrer à partir du menu déroulant **[Étiquette réseau]** , puis cliquez sur **[OK]** .

Commande d'E/S réseau

Les pools de ressources réseau déterminent la priorité accordée à différents types de trafic réseau sur un vDS.

Lorsqu'un contrôle d'E/S de réseau est activé, le trafic vDS est divisé en pools de ressources réseau suivants : trafic FT, trafic iSCSI, trafic vMotion, trafic de gestion, trafic NFS et trafic de machine virtuelle. Vous pouvez contrôler la priorité du trafic de chacun de ces pools de ressources réseau en définissant ses paramètres **[Partages adaptateurs physiques]** et **[Limites de l'hôte]** .

Les **[partages adaptateurs physiques]** assignés à un pool de ressources réseau déterminent le partage de la bande passante disponible totale accordée au trafic associé au pool de ressources réseau. Le partage de bande passante de transmission disponible pour un pool de ressources réseau dépend des partages du pool de ressources réseau et des données transmises par les autres pools de ressources réseau. Par exemple, si vous définissez vos pools de ressources du trafic FT et iSCSI à 100 partages, alors que chacun des autres pools de ressources est défini sur 50 partages, les pools de ressources du trafic FT et iSCSI reçoivent chacun 25 % de la bande passante disponible et les quatre pools de ressources restant. Les autres pools de ressources réseau reçoivent chacun 12,5 % de la bande passante disponible. Ces réservations s'appliquent uniquement lorsque la carte physique est saturée.

Remarque Les partages de pool de ressources de trafic iSCSI ne s'appliquent pas au trafic iSCSI d'un adapteur iSCSI matérielle dépendante.

La limite d'hôte **[Limite hôte]** d'un pool de ressources réseau est la limite supérieure de bande passante que le pool de ressources réseau peut utiliser.

Activer le contrôle d'E/S réseau sur un vDS

Autorisez la gestion des ressources réseau pour donner les priorités du trafic réseau en fonction de son type à l'aide des pools de ressources réseau.

Prérequis

Vérifiez qu'il y a au moins une version de commutateur distribué vNetwork version 4.1 sur votre centre de données.

Procédure

1 Dans vSphere Client, affichez la vue d'inventaire de réseau et sélectionnez le commutateur distribué vNetwork.

2 Sur l'onglet **[Allocation des ressources]** , cliquez sur **[Propriétés]** .

3 Sélectionnez **[Activer le réseau de gestion des ressources sur ce vDS]** et cliquez sur **[OK]** .

Modifier les paramètres de pool de ressources réseau

Vous pouvez modifier les paramètres de pool de ressources réseau, tels que les partages et les limites alloués pour chaque pool de ressources réseau.

Procédure

1 Dans vSphere Client, affichez la vue d'inventaire de réseau et sélectionnez le commutateur distribué vNetwork.

2 Dans l'onglet **[Allocation des ressources]** , cliquez avec le bouton droit sur le pool de ressources réseau à modifier et sélectionnez **[Modifier les paramètres]** .

3 Sélectionnez les partages de carte physique dans **[Partages adaptateurs physiques]** pour le pool de ressources réseau.

Option	Description
Personnalisé	Entrez un nombre spécifique de partages, de 1 à 100, pour ce pool de ressources réseau.
Haut	Définit les partages pour ce pool de ressources sur 100.
Normal	Définit les partages pour ce pool de ressources sur 50.
Bas	Définit les partages pour ce pool de ressources sur 25.

4 Définissez **[Limite hôte]** pour le pool de ressources réseau en mégabits par seconde ou sélectionnez **[Illimité]** .

5 Cliquez sur **[OK]** .

Mise en réseau avancée 5

La rubrique suivante vous guide à travers les étapes de mise en réseau avancée dans un environnement ESX, et vous explique comment configurer et modifier les options de configuration de mise en réseau avancée.

Ce chapitre aborde les rubriques suivantes :

Protocole Internet Version 6

vSphere prend en charge les environnements de Protocole Internet version 4 (IPv4) et version 6 (IPv6).

L'IETF (Internet Engineering Task Force) a conçu IPv6 pour succéder à IPv4. L'adoption d'IPv6, en tant que protocole autonome et dans un environnement mélangé avec IPv4, se développe rapidement. Avec IPv6, vous pouvez utiliser les fonctionnalités de vSphere dans un environnement IPv6.

La différence majeure entre IPv4 et IPv6 est la longueur d'adresse. L'IPv6 utilise des adresses 128 bits plutôt que des adresses 32 bits employées par IPv4. Cela évite le problème de l'épuisement d'adresse présent avec IPv4 et élimine le besoin de traduction d'adresses réseau. Il existe d'autres différences notables, telles que les adresses locales de lien qui apparaissent lorsque l'interface est initialisée, les adresses qui sont définies par des annonces de routage et la capacité d'avoir de multiples adresse IPv6 sur une interface.

Une configuration spécifique IPv6 dans vSphere implique de fournir des adresses IPv6 en saisissant des adresses statiques ou en utilisant un schéma de configuration d'adresse automatique pour toutes les interfaces réseau vSphere appropriées.

Activer le support IPv6 sur un hôte ESX

Vous pouvez activer ou mettre hors tension un support IPv6 sur l'hôte. IPv6 est désactivé par défaut.

Procédure

1 Cliquez sur la flèche à côté du bouton **[inventaire]** dans la barre de navigation et sélectionnez **[Hôtes et clusters]** .

2 Choisissez l'hôte et cliquez sur l'onglet **[Configuration]** .

3 Cliquez sur le lien **[Mise en réseau]** sous Matériel.

4 Dans la vue Commutateur virtuel, cliquez sur le lien **[Propriétés]** .

5 Sélectionnez **[Activer support IPv6 sur système hôte]** et cliquez sur **[OK]** .

6 Redémarrez l'hôte.

Configuration VLAN

Les VLAN (LAN virtuels) permettent à un segment LAN physique unique d'être davantage segmenté de sorte que des groupes de travail de ports soient isolés les uns des autres comme s'ils se trouvaient sur des segments physiquement différents.

La configuration ESX avec les VLAN est recommandée pour les raisons suivantes.

- Intégration de l'hôte dans un environnement préexistant.
- Sécurisation du trafic réseau.
- Réduction de la congestion du trafic réseau.
- Le trafic iSCSI nécessite un réseau isolé.

Vous pouvez configurer les VLAN dans ESX avec trois méthodes : Balisage de commutateur externe (EST), Balisage de commutateur virtuel (VST) et Balisage d'invité virtuel (VGT).

Avec EST, tous les balisages VLAN de paquets sont exécutés sur le commutateur physique. Les adaptateurs réseau hôtes sont connectés aux ports d'accès sur le commutateur physique. Les groupes de ports connectés au commutateur virtuel doivent avoir leur ID VLAN réglée sur 0.

Avec VST, tous les balisages VLAN de paquets sont exécutés par le commutateur virtuel avant de quitter l'hôte. Les adaptateurs réseau hôtes doivent être connectés aux ports trunk sur le commutateur physique. Les groupes de ports connectés au commutateur virtuel doivent avoir une ID VLAN appropriée spécifiée.

Avec VGT, tous les balisages VLAN sont exécutés par la machine virtuelle. Les balises VLAN sont conservées entre la pile réseau de la machine virtuelle et le commutateur externe quand les trames passent par les commutateurs virtuels. Les ports de commutateur physique sont réglés sur le port trunk.

Remarque En utilisant VGT, vous devez avoir un pilote trunk 802.1Q VLAN installé sur la machine virtuelle.

Règles de mise en réseau

Les règles configurées au niveau du groupes dvPort ou du commutateur vSwitch s'appliquent à tous les groupes de travail de ports sur ce vSwitch ou aux dvPort dans le groupes dvPort, à l'exclusion des options de configuration qui sont remplacées au niveau du dvPort ou du groupes de ports.

Vous pouvez appliquer les règles de mise en réseau suivantes.

- Basculement et équilibrage de charge
- VLAN (commutateur distribué vNetwork uniquement)

- Sécurité
- Formation du trafic
- Règles de blocage de ports (commutateur distribué vNetwork uniquement)

Règle de basculement et d'équilibrage de charge

Les règles de basculement et d'équilibrage de charge permettent de déterminer la répartition du trafic réseau entre les cartes et de réacheminer le trafic en cas d'échec d'un adapteur.

Vous pouvez modifier la règle de basculement et d'équilibrage de charge en configurant les paramètres suivants :

- **[Règle d'équilibrage de charge]** détermine la distribution du trafic sortant entre les adaptateurs réseau assignés à un commutateur vSwitch.

  REMARQUE Le trafic entrant est contrôlé par la règle d'équilibrage de charge sur le commutateur physique.

- **[Détection reprise]** contrôle l'état de lien et le sondage de balise. La signalisation n'est pas pris en charge par le balisage VLAN invité.
- **[Commande adaptateur réseau]** peut être actif ou en veille.

Modifier la règle de basculement et d'équilibrage de charge sur un commutateur vSwitch

Les règles de basculement et d'équilibrage de charge permettent de déterminer la répartition du trafic réseau entre les cartes et de réacheminer le trafic en cas d'échec d'un adapteur.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** , puis sur **[Mise en réseau]** .

3 Sélectionnez un commutateur vSwitch et cliquez sur **[Propriétés]** .

4 Dans la boîte de dialogue Propriétés de vSwitch, cliquez sur l'onglet **[Ports]** .

5 Pour modifier les valeurs de basculement et d'équilibrage de charge du commutateur vSwitch, sélectionnez l'élément vSwith et cliquez sur **[Propriétés]** .

6 Cliquez sur l'onglet **[Association de cartes réseau]** .

  Vous pouvez remplacer l'ordre de basculement au niveau du groupes de ports. Par défaut, les nouveaux adaptateurs sont actifs pour toutes les règles. Les nouveaux adaptateurs transportent le trafic pour le commutateur vSwitch et son groupes de ports, sauf indication contraire.

7 Spécifiez les paramètres dans le groupes d'exceptions à la règle.

Option	Description
Équilibrage de charge	Spécifiez comment choisir une liaison montante. ■ **[Route basée sur l'ID du port d'origine]** . Choisissez une liaison montante en fonction du port virtuel par lequel le trafic est entré dans le commutateur virtuel. ■ **[Route basée sur le hachage IP]** . Choisissez une liaison montante en fonction d'un hachage des adresses IP de source et de destination de chaque paquet. Pour les paquets non IP, les éléments présents à ces positions servent à calculer le hachage. ■ **[Route basée sur le hachage MAC source]** . Choisissez une liaison montante en fonction d'un hachage de l'Ethernet source. ■ **[Utiliser la commande de basculement explicite]** . Toujours utiliser la liaison montante d'ordre supérieur dans la liste des adaptateurs actifs qui vérifient les critères de détection du basculement. **REMARQUE** L'association basée sur IP exige que le commutateur physique soit configuré avec etherchannel. Pour toutes les autres options, etherchannel doit être désactivé.
Détection de basculement de réseau	Spécifiez la méthode pour l'utiliser pour la détection de basculement. ■ **[État de lien seulement]** . Repose uniquement sur l'état du lien fourni par l'adaptateur réseau. Cette option détecte les défaillances, telles que les débranchements de câble et les défaillances d'alimentation de commutateurs physiques, mais pas les erreurs de configuration, comme un port physique de commutateur bloqué par Spanning tree ou configuré vers un VLAN incorrect ou des débranchements de câble de l'autre côté d'un commutateur physique. ■ **[Sondage balise]** . Envoie et détecte des sondes de balise sur toutes les cartes réseau de l'association et utilise cette information, reliée à l'état du lien, pour déterminer les défaillances de liens. Ceci détecte plusieurs des échecs précédemment mentionnés qui ne sont pas détectés par l'état du lien seulement.
Notifier les commutateurs	Sélectionnez **[Oui]** ou **[Non]** pour notifier les commutateurs en cas de basculement. Si vous sélectionnez **[Oui]** , chaque fois qu'une carte réseau virtuelle est connecté au vSwitch ou chaque fois que le trafic de cette carte réseau virtuelle est acheminée par une autre carte réseau physique de l'association en raison d'un événement de basculement, une notification est envoyée sur le réseau pour mettre à niveau les tables de recherche sur les commutateurs physiques. Dans presque tous les cas, ce processus est souhaitable pour obtenir la plus basse latence dans les occurrences de basculement et les migrations avec vMotion. **REMARQUE** N'utilisez pas cette option quand les machines virtuelles utilisant le groupes de ports utilisent l'équilibrage de charge réseau Microsoft dans le mode monodiffusion. Ce problème n'existe pas lorsque NLB fonctionne en mode multidiffusion.

Option	Description
Retour arrière	Sélectionnez **[Oui]** ou **[Non]** pour mettre hors tension ou activer le retour arrière. Cette option détermine le mode de retour en activité d'un adaptateur physique lors de la récupération après échec. Si le retour arrière est défini sur **[Oui]** , la carte est ramenée au service actif immédiatement après la récupération, en déplaçant la carte de réserve qui a occupé son slot le cas échéant. Si le retour arrière est défini sur **[Non]** , un adapteur défectueuse est laissé inactive, même après la récupération, jusqu'à ce qu'une autre carte actuellement active échoue, exigeant son remplacement.
ordre de basculement	Spécifiez comment répartir la charge de travail pour les liaisons montantes. Si vous voulez utiliser certaines liaisons montantes mais en réservez d'autres pour les urgences si des liaisons montantes en cours d'utilisation échouent, définissez cette condition en les déplaçant dans différents groupes : ■ **[Liaisons montantes actives]** . Continuez à utiliser la liaison montante si la connectivité de l'adaptateur réseau est disponible et en activité. ■ **[Liaisons montantes en attente]** . Utilisez cette liaison montante si la connectivité d'un adaptateur actif est indisponible. ■ **[Liaisons montantes inutilisées]** . N'utilisez pas cette liaison montante.

8 Cliquez sur **[OK]** .

Modifier la règle de basculement et d'équilibrage de charge sur un groupes de ports

Les règles de basculement et d'équilibrage de charge permettent de déterminer la répartition du trafic réseau entre les cartes et de réacheminer le trafic en cas d'échec d'un adapteur.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Mise en réseau]** .

3 Sélectionnez un groupes de ports et cliquez sur **[Modifier]** .

4 Dans la boîte de dialogue Propriétés, cliquez sur l'onglet **[Ports]** .

5 Pour éditer les valeurs **[Basculement et équilibrage de charge]** du groupe de ports, sélectionnez le groupe de ports et cliquez sur **[Propriétés]** .

6 Cliquez sur l'onglet **[Association de cartes réseau]** .

Vous pouvez remplacer l'ordre de basculement au niveau du groupes de ports. Par défaut, les nouveaux adaptateurs sont actifs pour toutes les règles. Les nouveaux adaptateurs transportent le trafic pour le commutateur vSwitch et son groupes de ports, sauf indication contraire.

7 Spécifiez les paramètres dans le groupes d'exceptions à la règle.

Option	Description
Équilibrage de charge	Spécifiez comment choisir une liaison montante. ■ **[Route basée sur l'ID du port d'origine]** . Choisissez une liaison montante en fonction du port virtuel par lequel le trafic est entré dans le commutateur virtuel. ■ **[Route basée sur le hachage IP]** . Choisissez une liaison montante en fonction d'un hachage des adresses IP de source et de destination de chaque paquet. Pour les paquets non IP, les éléments présents à ces positions servent à calculer le hachage. ■ **[Route basée sur le hachage MAC source]** . Choisissez une liaison montante en fonction d'un hachage de l'Ethernet source. ■ **[Utiliser la commande de basculement explicite]** . Toujours utiliser la liaison montante d'ordre supérieur dans la liste des adaptateurs actifs qui vérifient les critères de détection du basculement. **Remarque** L'association basée sur IP exige que le commutateur physique soit configuré avec etherchannel. Pour toutes les autres options, etherchannel doit être désactivé.
Détection de basculement de réseau	Spécifiez la méthode pour l'utiliser pour la détection de basculement. ■ **[État de lien seulement]** . Repose uniquement sur l'état du lien fourni par l'adaptateur réseau. Cette option détecte les défaillances, telles que les débranchements de câble et les défaillances d'alimentation de commutateurs physiques, mais pas les erreurs de configuration, comme un port physique de commutateur bloqué par Spanning tree ou configuré vers un VLAN incorrect ou des débranchements de câble de l'autre côté d'un commutateur physique. ■ **[Sondage balise]** . Envoie et détecte des sondes de balise sur toutes les cartes réseau de l'association et utilise cette information, reliée à l'état du lien, pour déterminer les défaillances de liens. Ceci détecte plusieurs des échecs précédemment mentionnés qui ne sont pas détectés par l'état du lien seulement.
Notifier les commutateurs	Sélectionnez **[Oui]** ou **[Non]** pour notifier les commutateurs en cas de basculement. Si vous sélectionnez **[Oui]** , chaque fois qu'une carte réseau virtuelle est connecté au vSwitch ou chaque fois que le trafic de cette carte réseau virtuelle est acheminée par une autre carte réseau physique de l'association en raison d'un événement de basculement, une notification est envoyée sur le réseau pour mettre à niveau les tables de recherche sur les commutateurs physiques. Dans presque tous les cas, ce processus est souhaitable pour obtenir la plus basse latence dans les occurrences de basculement et les migrations avec vMotion. **Remarque** N'utilisez pas cette option quand les machines virtuelles utilisant le groupes de ports utilisent l'équilibrage de charge réseau Microsoft dans le mode monodiffusion. Ce problème n'existe pas lorsque NLB fonctionne en mode multidiffusion.

Option	Description
Retour arrière	Sélectionnez **[Oui]** ou **[Non]** pour mettre hors tension ou activer le retour arrière. Cette option détermine le mode de retour en activité d'un adaptateur physique lors de la récupération après échec. Si le retour arrière est défini sur **[Oui]** , la carte est ramenée au service actif immédiatement après la récupération, en déplaçant la carte de réserve qui a occupé son slot le cas échéant. Si le retour arrière est défini sur **[Non]** , un adapteur défectueuse est laissé inactive, même après la récupération, jusqu'à ce qu'une autre carte actuellement active échoue, exigeant son remplacement.
ordre de basculement	Spécifiez comment répartir la charge de travail pour les liaisons montantes. Si vous voulez utiliser certaines liaisons montantes mais en réservez d'autres pour les urgences si des liaisons montantes en cours d'utilisation échouent, définissez cette condition en les déplaçant dans différents groupes : ■ **[Liaisons montantes actives]** . Continuez à utiliser la liaison montante si la connectivité de l'adaptateur réseau est disponible et en activité. ■ **[Liaisons montantes en attente]** . Utilisez cette liaison montante si la connectivité d'un adaptateur actif est indisponible. ■ **[Liaisons montantes inutilisées]** . N'utilisez pas cette liaison montante.

8 Cliquez sur **[OK]** .

Modifier la règle d'association et de basculement sur un groupes dvPort

Les règles Teaming and Failover permettent de déterminer la répartition du trafic réseau entre les cartes et de réacheminer le trafic en cas d'échec d'un adapteur.

Procédure

1 Dans vSphere Client, affichez la vue d'inventaire Mise en réseau et sélectionnez le groupes dvPort.

2 Dans le menu Inventaire, sélectionnez **[Réseau] > [Modifier les paramètres]** .

3 Sélectionnez **[Règles]** .

4 Dans le groupes Teaming and Failover, spécifiez les éléments suivants.

Option	Description
Équilibrage de charge	Spécifiez comment choisir une liaison montante. ■ **[Route basée sur ID port d'origine]** : choisissez une liaison montante basée sur le port virtuel par lequel est entré le trafic dans le commutateur virtuel. ■ **[Route basée sur le hachage IP]** : choisissez une liaison montante en fonction d'un hachage des adresses IP source et de destination de chaque paquet. Pour les paquets non IP, les éléments présents à ces positions servent à calculer le hachage. ■ **[Route basée sur hachage MAC source]** : choisissez une liaison montante en fonction d'un hachage de l'Ethernet source. ■ **[Route basée sur la charge NIC physique]** — Choisissez une liaison montante basée sur les charges actuelles des NIC physiques. ■ **[Utiliser la commande de basculement explicite]** : Utilisez toujours la liaison montante d'ordre supérieur dans la liste des cartes actives qui satisfait les critères de détection de basculement. **Remarque** L'association basée sur IP exige que le commutateur physique soit configuré avec etherchannel. Pour toutes les autres options, etherchannel doit être désactivé.
Détection de basculement de réseau	Spécifiez la méthode pour l'utiliser pour la détection de basculement. ■ **[État de lien seulement]** : basée uniquement sur l'état du lien que la carte réseau fournit. Cette option détecte les défaillances, telles que les débranchements de câble et les défaillances d'alimentation de commutateurs physiques, mais pas les erreurs de configuration, comme un port physique de commutateur bloqué par Spanning tree ou configuré vers un VLAN incorrect ou des débranchements de câble de l'autre côté d'un commutateur physique. ■ **[Sondage balise]** : envoie et écoute des sondes de balise sur toutes les cartes réseau dans l'association et emploie ces informations, en plus de l'état de lien, pour déterminer l'échec du lien. Ceci détecte plusieurs des échecs précédemment mentionnés qui ne sont pas détectés par l'état du lien seulement. **Remarque** Ne choisissez pas le sondage de balise avec l'équilibrage de charge avec hachage IP.
Notifier les commutateurs	Sélectionnez **[Oui]** ou **[Non]** pour notifier les commutateurs en cas de basculement. Si vous sélectionnez **[Oui]** , chaque fois qu'un adaptateur réseau virtuelle est connecté au vSwitch ou chaque fois que le trafic de cette carte réseau virtuelle est acheminé par une autre carte réseau physique de l'association en raison d'un événement de basculement, une notification est envoyée sur le réseau pour mettre à niveau les tables de recherche sur les commutateurs physiques. Dans presque tous les cas, ce processus est souhaitable pour obtenir la plus basse latence dans les occurrences de basculement et les migrations avec vMotion. **Remarque** N'utilisez pas cette option quand les machines virtuelles utilisant le groupes de ports utilisent l'équilibrage de charge réseau Microsoft dans le mode monodiffusion. Ce problème n'existe pas lorsque NLB fonctionne en mode multidiffusion.

Option	Description
Retour arrière	Sélectionnez **[Oui]** ou **[Non]** pour mettre hors tension ou activer le retour arrière. Cette option détermine le mode de retour en activité d'un adaptateur physique lors de la récupération après échec. Si le retour arrière est défini sur **[Oui]** , la carte est ramenée au service actif immédiatement après la récupération, en déplaçant la carte de réserve qui a occupé son slot le cas échéant. Si le retour arrière est défini sur **[Non]** , un adapteur défectueuse est laissé inactive, même après la récupération, jusqu'à ce qu'une autre carte actuellement active échoue, exigeant son remplacement.
ordre de basculement	Spécifiez comment répartir la charge de travail pour les liaisons montantes. Si vous voulez utiliser certaines liaisons montantes mais en réserver d'autres pour les urgences si des liaisons montantes en cours d'utilisation échouent, définissez cette condition en les déplaçant dans différents groupes : ■ **[liaison montante active]** : continuez à utiliser la liaison montante quand la connectivité de la carte réseau est active. ■ **[Liaisons montantes de réserve]** — Utilisez cette liaison montante si la connectivité d'une des cartes actives est coupée. ■ **[Liaisons montantes inutilisés]** : n'utilisez pas cette liaison montante. **Remarque** En utilisant l'équilibrage de charge pas hachage IP, ne configurez pas les liaisons montantes de réserve.

5 Cliquez sur **[OK]** .

Modifier les règles d'association de dvPort et de basculement

Les règles Teaming and Failover permettent de déterminer la répartition du trafic réseau entre les cartes et de réacheminer le trafic en cas d'échec d'un adapteur.

Prérequis

Pour modifier les règles d'association et de basculement sur un dvPort individuel, le groupes dvPort associé doit être paramétré pour autoriser les remplacements de règles.

Procédure

1 Ouvrez une session sur vSphere Client et affichez le commutateur distribué vNetwork.

2 Dans l'onglet **[Ports]** , cliquez avec le bouton droit sur le port à modifier et sélectionnez **[Modifier les paramètres]** .

La boîte de dialogue **[Paramétrages port]** apparaît.

3 Cliquez sur **[Règles]** pour afficher et modifier les règles de réseau des ports.

4 Dans le groupes Teaming and Failover, spécifiez les éléments suivants.

Option	Description
Équilibrage de charge	Spécifiez comment choisir une liaison montante. ■ **[Route basée sur ID port d'origine]** : choisissez une liaison montante basée sur le port virtuel par lequel est entré le trafic dans le commutateur virtuel. ■ **[Route basée sur le hachage IP]** : choisissez une liaison montante en fonction d'un hachage des adresses IP source et de destination de chaque paquet. Pour les paquets non IP, les éléments présents à ces positions servent à calculer le hachage. ■ **[Route basée sur hachage MAC source]** : choisissez une liaison montante en fonction d'un hachage de l'Ethernet source. ■ **[Route basée sur la charge NIC physique]** — Choisissez une liaison montante basée sur les charges actuelles des NIC physiques. ■ **[Utiliser la commande de basculement explicite]** : Utilisez toujours la liaison montante d'ordre supérieur dans la liste des cartes actives qui satisfait les critères de détection de basculement. **Remarque** L'association basée sur IP exige que le commutateur physique soit configuré avec etherchannel. Pour toutes les autres options, etherchannel doit être désactivé.
Détection de basculement de réseau	Spécifiez la méthode pour l'utiliser pour la détection de basculement. ■ **[État de lien seulement]** : basée uniquement sur l'état du lien que la carte réseau fournit. Cette option détecte les défaillances, telles que les débranchements de câble et les défaillances d'alimentation de commutateurs physiques, mais pas les erreurs de configuration, comme un port physique de commutateur bloqué par Spanning tree ou configuré vers un VLAN incorrect ou des débranchements de câble de l'autre côté d'un commutateur physique. ■ **[Sondage balise]** : envoie et écoute des sondes de balise sur toutes les cartes réseau dans l'association et emploie ces informations, en plus de l'état de lien, pour déterminer l'échec du lien. Ceci détecte plusieurs des échecs précédemment mentionnés qui ne sont pas détectés par l'état du lien seulement. **Remarque** Ne choisissez pas le sondage de balise avec l'équilibrage de charge avec hachage IP.
Notifier les commutateurs	Sélectionnez **[Oui]** ou **[Non]** pour notifier les commutateurs en cas de basculement. Si vous sélectionnez **[Oui]** , chaque fois qu'un adaptateur réseau virtuelle est connecté au vSwitch ou chaque fois que le trafic de cette carte réseau virtuelle est acheminé par une autre carte réseau physique de l'association en raison d'un événement de basculement, une notification est envoyée sur le réseau pour mettre à niveau les tables de recherche sur les commutateurs physiques. Dans presque tous les cas, ce processus est souhaitable pour obtenir la plus basse latence dans les occurrences de basculement et les migrations avec vMotion. **Remarque** N'utilisez pas cette option quand les machines virtuelles utilisant le groupes de ports utilisent l'équilibrage de charge réseau Microsoft dans le mode monodiffusion. Ce problème n'existe pas lorsque NLB fonctionne en mode multidiffusion.

Option	Description
Retour arrière	Sélectionnez **[Oui]** ou **[Non]** pour mettre hors tension ou activer le retour arrière. Cette option détermine le mode de retour en activité d'un adaptateur physique lors de la récupération après échec. Si le retour arrière est défini sur **[Oui]** , la carte est ramenée au service actif immédiatement après la récupération, en déplaçant la carte de réserve qui a occupé son slot le cas échéant. Si le retour arrière est défini sur **[Non]** , un adapteur défectueuse est laissé inactive, même après la récupération, jusqu'à ce qu'une autre carte actuellement active échoue, exigeant son remplacement.
ordre de basculement	Spécifiez comment répartir la charge de travail pour les liaisons montantes. Si vous voulez utiliser certaines liaisons montantes mais en réserver d'autres pour les urgences si des liaisons montantes en cours d'utilisation échouent, définissez cette condition en les déplaçant dans différents groupes : ■ **[liaison montante active]** : continuez à utiliser la liaison montante quand la connectivité de la carte réseau est active. ■ **[Liaisons montantes de réserve]** — Utilisez cette liaison montante si la connectivité d'une des cartes actives est coupée. ■ **[Liaisons montantes inutilisés]** : n'utilisez pas cette liaison montante. **Remarque** En utilisant l'équilibrage de charge pas hachage IP, ne configurez pas les liaisons montantes de réserve.

5 Cliquez sur **[OK]** .

Règle VLAN

La règle de VLAN permet aux réseaux virtuels de joindre des VLAN physiques.

Modifier la règle VLAN sur un groupes dvPort

Vous pouvez modifier la configuration de la règle VLAN sur un groupes dvPort.

Procédure

1 Dans vSphere Client, affichez la vue d'inventaire Mise en réseau et sélectionnez le groupes dvPort.

2 Dans le menu Inventaire, sélectionnez **[Réseau]** > **[Modifier les paramètres]** .

3 Sélectionnez **[VLAN]** .

4 Sélectionnez le type de VLAN **[VLAN Type]** à utiliser.

Option	Description
Aucune	N'utilise pas de VLAN.
VLAN	Dans le champ **[ID VLAN]** , entrez un nombre entre 1 et 4094.
jonction VLAN	Entrez une plage de jonctions VLAN dans **[Intervalle de joncteur réseau VLAN]** .
VLAN privé	Sélectionnez un VLAN privé disponible à utiliser.

Modifier les règles VLAN du dvPort

Une règle VLAN définie au niveau du dvPort permet au dvPort individuel de remplacer la règle VLAN définie au niveau du groupes dvPort.

Prérequis

Pour modifier les règles VLAN sur un dvPort individuel, le groupes dvPort associé doit être paramétré pour autoriser les remplacements de règles.

Procédure

1 Ouvrez une session sur vSphere Client et affichez le commutateur distribué vNetwork.

2 Dans l'onglet **[Ports]** , cliquez avec le bouton droit sur le port à modifier et sélectionnez **[Modifier les paramètres]** .

3 Cliquez sur **[Règles]** .

4 Sélectionnez le type de VLAN à utiliser.

Option	Action
Aucune	Ne pas utiliser de VLAN.
VLAN	Dans le champ VLAN ID, entrez un nombre entre 1 et 4095.
jonction VLAN	Entrez une plage de jonctions VLAN.
VLAN privé	Sélectionnez un VLAN privé disponible à utiliser.

5 Cliquez sur **[OK]** .

Règle de sécurité

Les règles de sécurité réseau déterminent la façon dont la carte filtre les trames entrantes et sortantes.

La couche 2 est la couche de liaison de données. Les trois éléments de la règle de sécurité sont le mode promiscuité, les changements d'adresse MAC et les Transmissions forgées.

En mode non-promiscuité, un adapteur invitée écoute uniquement le trafic transféré sur sa propre adresse MAC. En mode promiscuité, elle peut écouter l'ensemble des trames. Par défaut, les cartes invitées sont configurées sur le mode non-promiscuité.

Modifier la règle de sécurité de la couche 2 sur un commutateur vSwitch

Contrôlez la gestion de trames entrantes et sortantes en modifiant les règles de sécurité de la couche 2.

Procédure

1 Ouvrez une session sur VMware vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** , puis sur **[Mise en réseau]** .

3 Cliquez sur **[Propriétés]** pour le commutateur vSwitch à modifier.

4 Dans la boîte de dialogue Propriétés, cliquez sur l'onglet **[Ports]** .

5 Sélectionnez l'élément vSwitch et cliquez sur **[Modifier]** .

6 Dans la boîte de dialogue Propriétés, cliquez sur l'onglet **[Sécurité]** .

Par défaut, le mode **[Mode promiscuité :]** est défini sur **[Rejeter]** ; **[Modifications d'adresse MAC]** et **[Transmissions forcées :]** sont définis sur **[Accepter]** .

La règle s'applique à toutes les cartes virtuelles sur le commutateur vSwitch excepté quand le groupes de ports pour la carte virtuelle spécifie une exception à la règle.

7 Dans le volet Exceptions règle, choisissez de rejeter ou d'accepter les exceptions à la règle de sécurité.

Tableau 5-1. Exceptions de règle

Mode	Rejeter	Accepter
Mode promiscuité	Une carte invitée en mode promiscuité n'a aucun effet sur la réception des trames qu'elle reçoit.	Une carte invitée en mode promiscuité détecte toutes les trames transmises au vSwitch qui sont autorisées par la règle VLAN pour le groupes de ports auquel est connectée la carte.
Modifications d'adresse MAC	Si le système d'exploitation invité modifie l'adresse MAC de la carte par une autre ne figurant pas dans le fichier de configuration `.vmx`, toutes les trames entrantes sont supprimées. Si le système d'exploitation invité rechange l'adresse MAC pour qu'elle corresponde à l'adresse MAC figurant dans le fichier de configuration `.vmx`, les trames entrantes sont de nouveau envoyées.	Si l'adresse MAC du système d'exploitation invité change, les trames pour la nouvelle adresse MAC sont reçues.
Transmissions forgées	Toutes les trames sortantes dont l'adresse MAC source diffère de celle définie sur la carte sont supprimées.	Aucun filtrage n'est exécuté et toutes les trames sortantes sont transmises.

8 Cliquez sur **[OK]** .

Modifier l'exception à la règle de sécurité de la couche 2 sur un groupes de ports

Contrôlez la gestion de trames entrantes et sortantes en modifiant les règles de sécurité de la couche 2.

Procédure

1 Ouvrez une session sur VMware vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** , puis sur **[Mise en réseau]** .

3 Cliquez sur **[Propriétés]** pour le groupes de ports à modifier.

4 Dans la boîte de dialogue Propriétés, cliquez sur l'onglet **[Ports]** .

5 Sélectionnez l'élément de groupes de ports et cliquez sur **[Modifier]** .

6 Dans la boîte de dialogue Propriétés pour le groupes de ports, cliquez sur l'onglet **[Sécurité]** .

Par défaut, **[Mode promiscuité]** est défini sur **[Rejeter]** . **[Modifications d'adresse MAC]** et **[Transmissions forcées :]** sont définis sur **[Accepter]** .

L'exception à la règle remplace toute règle définie au niveau du commutateur vSwitch.

7 Dans le volet Exceptions règle, choisissez de rejeter ou d'accepter les exceptions à la règle de sécurité.

Tableau 5-2. Exceptions de règle

Mode	Rejeter	Accepter
Mode promiscuité	Une carte invitée en mode promiscuité n'a aucun effet sur la réception des trames qu'elle reçoit.	Une carte invitée en mode promiscuité détecte toutes les trames transmises au vSwitch qui sont autorisées par la règle VLAN pour le groupes de ports auquel est connectée la carte.
Modifications d'adresse MAC	Si le système d'exploitation invité modifie l'adresse MAC de la carte par une autre ne figurant pas dans le fichier de configuration `.vmx`, toutes les trames entrantes sont supprimées. Si le système d'exploitation invité rechange l'adresse MAC pour qu'elle corresponde à l'adresse MAC figurant dans le fichier de configuration `.vmx`, les trames entrantes sont de nouveau envoyées.	Si l'adresse MAC du système d'exploitation invité change, les trames pour la nouvelle adresse MAC sont reçues.
Transmissions forgées	Toutes les trames sortantes dont l'adresse MAC source diffère de celle définie sur la carte sont supprimées.	Aucun filtrage n'est exécuté et toutes les trames sortantes sont transmises.

8 Cliquez sur **[OK]** .

Modifier la règle de sécurité sur un groupes dvPort

Contrôlez la gestion des trames entrantes et sortantes pour un groupes dvPort en modifiant les règles de sécurité.

Procédure

1 Dans vSphere Client, affichez la vue d'inventaire Mise en réseau et sélectionnez le groupes dvPort.

2 Dans le menu Inventaire, sélectionnez **[Réseau]** > **[Modifier les paramètres]** .

3 Dans la boîte de dialogue Propriétés pour le groupes de ports, cliquez sur l'onglet **[Sécurité]** .

Par défaut, **[Mode promiscuité]** est défini sur **[Rejeter]** . **[Modifications d'adresse MAC]** et **[Transmissions forcées :]** sont définis sur **[Accepter]** .

L'exception à la règle remplace toute règle définie au niveau du commutateur vSwitch.

4 Dans le volet Exceptions règle, choisissez de rejeter ou d'accepter les exceptions à la règle de sécurité.

Tableau 5-3. Exceptions de règle

Mode	Rejeter	Accepter
Mode promiscuité	Une carte invitée en mode promiscuité n'a aucun effet sur la réception des trames qu'elle reçoit.	Une carte invitée en mode promiscuité détecte toutes les trames transmises au vSwitch qui sont autorisées par la règle VLAN pour le groupes de ports auquel est connectée la carte.
Modifications d'adresse MAC	Si le système d'exploitation invité modifie l'adresse MAC de la carte par une autre ne figurant pas dans le fichier de configuration `.vmx`, toutes les trames entrantes sont supprimées. Si le système d'exploitation invité rechange l'adresse MAC pour qu'elle corresponde à l'adresse MAC figurant dans le fichier de configuration `.vmx`, les trames entrantes sont de nouveau envoyées.	Si l'adresse MAC du système d'exploitation invité change, les trames pour la nouvelle adresse MAC sont reçues.
Transmissions forgées	Toutes les trames sortantes dont l'adresse MAC source diffère de celle définie sur la carte sont supprimées.	Aucun filtrage n'est exécuté et toutes les trames sortantes sont transmises.

5 Cliquez sur **[OK]** .

Modifier les règles de sécurité du dvPort

Contrôlez la gestion des trames entrantes et sortantes pour un dvPort en modifiant les règles de sécurité.

Prérequis

Pour modifier les règles de sécurité sur un dvPort individuel, le groupes dvPort associé doit être paramétré pour autoriser les remplacements de règles.

Procédure

1 Ouvrez une session sur vSphere Client et affichez le commutateur distribué vNetwork.

2 Dans l'onglet **[Ports]** , cliquez avec le bouton droit sur le port à modifier et sélectionnez **[Modifier les paramètres]** .

3 Cliquez sur **[Règles]** .

Par défaut, le mode **[Mode promiscuité :]** est défini sur **[Rejeter]** ; **[Modifications d'adresse MAC]** et **[Transmissions forcées]** sont définis sur **[Accepter]** .

4 Dans le groupes Sécurité, choisissez de rejeter ou d'accepter les exceptions aux règles de sécurité.

Tableau 5-4. Exceptions

Mode	Rejeter	Accepter
Mode promiscuité	Une carte invitée en mode promiscuité n'a aucun effet sur la réception des trames qu'elle reçoit.	Une carte invitée en mode promiscuité détecte toutes les trames transmises au vSwitch qui sont autorisées par la règle VLAN pour le groupes de ports auquel est connectée la carte.
Modifications d'adresse MAC	Si le système d'exploitation invité modifie l'adresse MAC de la carte par une autre ne figurant pas dans le fichier de configuration `.vmx`, toutes les trames entrantes sont supprimées. Si le système d'exploitation invité rechange l'adresse MAC pour qu'elle corresponde à l'adresse MAC figurant dans le fichier de configuration `.vmx`, les trames entrantes sont de nouveau envoyées.	Si l'adresse MAC du système d'exploitation invité change, les trames pour la nouvelle adresse MAC sont reçues.
Transmissions forgées	Toutes les trames sortantes dont l'adresse MAC source diffère de celle définie sur la carte sont supprimées.	Aucun filtrage n'est exécuté et toutes les trames sortantes sont transmises.

5 Cliquez sur **[OK]** .

Règle de formation du trafic

Une règle de formation du trafic est définie par les trois caractéristiques suivantes : bande passante moyenne, bande passante maximale et taille de rafale. Vous pouvez établir une règle de formation du trafic pour chaque groupes de ports et chaque dvPort ou groupes dvPort.

ESX contrôle le trafic du réseau sortant sur des commutateurs vSwitch, et le trafic entrant et sortant sur un commutateur distribué vNetwork. La formation du trafic limite la bande passante de réseau à la disposition d'un port, mais elle peut également être configurée pour permettre à des rafales du trafic de traverser à des vitesses plus élevées.

Bande passante moyenne Établit le nombre de bits par seconde à autoriser sur un port, en moyenne dans le temps : charge moyenne autorisée.

Bande passante maximale Nombre maximal d'octets par seconde à autoriser à travers un port quand il reçoit ou envoie une rafale de trafic. Ce paramètre limite la bande passante utilisée par un port lorsqu'il utilise son bonus de rafale.

Taille de rafale Nombre maximal d'octets à autoriser dans une rafale. Si ce paramètre est défini, un port peut obtenir un bonus de rafale s'il n'utilise pas toute sa bande passante allouée. Chaque fois que le port a besoin de plus de bande passante que la quantité spécifiée par **[Bande passante moyenne]** , il peut être autorisé à transmettre temporairement des données à une vitesse plus élevée si un bonus de rafale est disponible. Ce paramètre limite le nombre d'octets qui peuvent être cumulés dans le bonus de rafale et ainsi transférés à une vitesse plus élevée.

Modifier la règle de formation du trafic sur un commutateur vSwitch

Utilisez les règles de formation du trafic pour contrôler la taille de la bande passante et des rafales sur un commutateur vSwitch.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** , puis sur **[Mise en réseau]** .

3 Cliquez sur **[Propriétés]** pour le commutateur vSwitch à modifier.

4 Dans la boîte de dialogue Propriétés, cliquez sur l'onglet **[Ports]** .

5 Sélectionnez l'élément vSwitch et cliquez sur **[Modifier]** .

6 Dans la boîte de dialogue Propriétés, cliquez sur l'onglet **[Formation du trafic]** .

Quand la formation du trafic est désactivée, les options sont grisées. Vous pouvez remplacer de manière sélective toutes les fonctionnalités de formation du trafic au niveau du groupes de ports, si la formation du trafic est activée.

Cette règle est appliquée à chaque carte virtuelle individuelle reliée au groupes de ports, et non au commutateur vSwitch dans son ensemble.

Remarque La bande passante maximale ne peut pas être inférieure à la bande passante moyenne spécifiée.

Option	Description
État	Si vous activez l'exception à la règle dans le champ **[État]** , vous limitez l'allocation de bande passante réseau pour chaque carte virtuelle associée à ce groupes de ports particulier. Si vous désactivez la règle, les services ont une connexion libre et claire au réseau physique.
Bande passante moyenne	Valeur mesurée sur une période de temps spécifique.
Bande passante maximale	Limite la bande passante maximale au cours de la rafale. Elle doit toujours être supérieure à la bande passante moyenne.
Taille de rafale	Spécifie la capacité d'une rafale en kilooctets (ko).

Modifier la règle de formation du trafic sur un groupes de ports

Utilisez les règles de formation du trafic pour contrôler la taille de la bande passante et des rafales sur un groupes de ports.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** , puis sur **[Mise en réseau]** .

3 Cliquez sur **[Propriétés]** pour le groupes de ports à modifier.

4 Dans la boîte de dialogue Propriétés, cliquez sur l'onglet **[Ports]** .

5 Sélectionnez l'élément de groupes de ports et cliquez sur **[Modifier]** .

6 Dans la boîte de dialogue Propriétés pour le groupes de ports, cliquez sur l'onglet **[Formation du trafic]** .

Quand la formation du trafic est désactivée, les options sont grisées.

Option	Description
État	Si vous activez l'exception à la règle dans le champ **[État]** , vous limitez l'allocation de bande passante réseau pour chaque carte virtuelle associée à ce groupes de ports particulier. Si vous désactivez la règle, les services ont une connexion libre et claire au réseau physique.
Bande passante moyenne	Valeur mesurée sur une période de temps spécifique.
Bande passante maximale	Limite la bande passante maximale au cours de la rafale. Elle doit toujours être supérieure à la bande passante moyenne.
Taille de rafale	Spécifie la capacité d'une rafale en kilooctets (ko).

Modifier la règle de formation du trafic sur un groupes de dvPort

Vous pouvez contrôler le trafic entrant et sortant sur des commutateurs distribués vNetwork. Vous pouvez limiter la bande passante réseau disponible pour un port, et également autoriser temporairement les rafales de trafic à traverser un port à des vitesses plus élevées.

Une règle de formation du trafic est définie par les trois caractéristiques suivantes : bande passante moyenne, bande passante maximale et taille de rafale. Les règles de formation du trafic ne s'appliquent pas au trafic iSCSI sur un adaptateur matériel iSCSI dépendant.

Procédure

1 Dans vSphere Client, affichez la vue d'inventaire Mise en réseau et sélectionnez le groupes dvPort.

2 Dans le menu Inventaire, sélectionnez **[Réseau] > [Modifier les paramètres]** .

3 Sélectionnez **[Formation du trafic]** .

4 Dans la boîte de dialogue Propriétés pour le groupes de ports, cliquez sur l'onglet **[Formation du trafic]** .

Vous pouvez configurer la formation du trafic entrant et sortant. Quand la formation du trafic est désactivée, les options sont grisées.

Remarque La bande passante maximale ne peut pas être inférieure à la bande passante moyenne spécifiée.

Option	Description
État	Si vous activez l'exception à la règle dans le champ **[État]** , vous limitez l'allocation de bande passante réseau pour chaque carte virtuelle associée à ce groupes de ports particulier. Si vous désactivez la règle, les services ont une connexion libre et claire au réseau physique.
Bande passante moyenne	Valeur mesurée sur une période de temps spécifique.
Bande passante maximale	Limite la bande passante maximale au cours de la rafale. Elle doit toujours être supérieure à la bande passante moyenne.
Taille de rafale	Spécifie la capacité d'une rafale en kilooctets (ko).

Modifier les règles de formation du trafic du dvPort

Vous pouvez contrôler le trafic entrant et sortant sur des commutateurs distribués vNetwork. Vous pouvez limiter la bande passante réseau disponible pour un port, et également autoriser temporairement les rafales de trafic à traverser un port à des vitesses plus élevées.

Une règle de formation du trafic est définie par les trois caractéristiques suivantes : bande passante moyenne, bande passante maximale et taille de rafale. Les règles de formation du trafic ne s'appliquent pas au trafic iSCSI sur un adaptateur matériel iSCSI dépendant.

Prérequis

Pour modifier les règles de formation du trafic sur un dvPort individuel, le groupes dvPort associé doit être paramétré pour autoriser les remplacements de règles.

Procédure

1 Ouvrez une session sur vSphere Client et affichez le commutateur distribué vNetwork.

2 Sur l'onglet **[Ports]** , cliquez avec le bouton droit sur le port à modifier et sélectionnez **[Modifier les paramètres]** .

3 Cliquez sur **[Règles]** .

4 Dans le groupes de formation du trafic, vous pouvez configurer la formation du trafic entrant et sortant.

Quand la formation du trafic est désactivée, les options sont grisées.

Option	Description
État	Si vous activez l'exception à la règle dans le champ **[État]** , vous limitez l'allocation de bande passante réseau pour chaque carte virtuelle associée à ce groupes de ports particulier. Si vous désactivez la règle, les services ont une connexion libre et claire au réseau physique.
Bande passante moyenne	Valeur mesurée sur une période de temps spécifique.
Bande passante maximale	Limite la bande passante maximale au cours de la rafale. Elle doit toujours être supérieure à la bande passante moyenne.
Taille de rafale	Spécifie la capacité d'une rafale en kilooctets (ko).

5 Cliquez sur **[OK]** .

Règles de blocage des ports

Configurez les règles de blocage pour les dvPorts depuis la boîte de dialogue des règles diverses.

Modifier la règle de blocage des ports sur un groupes dvPort

Configurez la règle de blocage des ports pour un groupes dvPort sous les règles diverses.

Procédure

1 Dans vSphere Client, affichez la vue d'inventaire Mise en réseau et sélectionnez le groupes dvPort.

2 Dans le menu Inventaire, sélectionnez **[Réseau]** > **[Modifier les paramètres]** .

3 Sélectionnez **[Divers]** .

4 Choisissez de bloquer tous les ports avec **[Bloquer tous les ports]** sur ce groupes dvPort.

Modifier la règle de blocage des ports dvPort

La boîte de dialogue des règles diverses permet de configurer des règles de blocage de ports pour un dvPort.

Procédure

1 Ouvrez une session sur vSphere Client et affichez le commutateur distribué vNetwork.

2 Dans l'onglet **[Ports]** , cliquez avec le bouton droit sur le port à modifier et sélectionnez **[Modifier les paramètres]** .

3 Cliquez sur **[Règles]** .

4 Dans le groupes **[Divers]** , choisissez de bloquer ou non ce port avec **[Bloquer tous les ports]** .

5 Cliquez sur **[OK]** .

Changer les configurations de routage et DNS

Vous pouvez modifier les informations du serveur DNS ou de passerelle par défaut fournies lors de l'installation à la page de configuration de l'hôte dans vSphere Client.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.

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

3 À droite de la fenêtre, cliquez sur **[Propriétés]** .

4 Dans l'onglet **[Config. DNS]** , entrez un nom et un domaine.

5 Choisissez d'obtenir automatiquement l'adresse du serveur DNS ou d'utiliser une adresse du serveur DNS.

Remarque DHCP est pris en charge uniquement si le serveur DHCP est accessible à la console de service. L'interface virtuelle (vswif) de la console de service doit être configurée et reliée au réseau où réside le serveur DHCP.

---

6 Spécifiez les domaines de recherche d'hôtes.

7 Sur l'onglet **[Routage]** , modifiez les informations de passerelle par défaut, si nécessaire.

Sélectionnez un périphérique de passerelle uniquement si vous avez configuré la console de service pour qu'elle se connecte à plusieurs sous-réseaux.

8 Cliquez sur **[OK]** .

Adresses MAC

Les adresses MAC sont générées pour les cartes réseau virtuelles utilisées par la console du service, le VMkernel et les machines virtuelles.

Dans la plupart des cas, les adresses MAC générées sont appropriées. Néanmoins, vous devrez peut-être configurer une adresse MAC pour un adapteur réseau virtuelle, notamment dans les cas suivants :

- Les cartes réseau virtuelles sur différents hôtes physiques partagent le même sous-réseau et se voient assigner la même adresse MAC, ce qui provoque un conflit.
- Pour garantir que la carte réseau virtuelle ait toujours la même adresse MAC.

Pour contourner la limite des 256 cartes réseau virtuelles par machine physique et les conflits possibles d'adresse MAC entre machines virtuelles, les administrateurs système peuvent attribuer manuellement des adresses MAC. VMware utilise l'OUI (Organizationally Unique Identifier) 00:50:56 pour les adresses générées manuellement.

La plage d'adresses MAC est `00:50:56:00:00:00–00:50:56:3F:FF:FF`.

Vous pouvez configurer les adresses en ajoutant la ligne suivante dans le fichier de configuration d'une machine virtuelle :

```
ethernet<number>.address = 00:50:56:XX:YY:ZZ
```

où <*number*> est le numéro de la carte Ethernet, `XX` est un nombre hexadécimal valide entre 00 et 3F, et `YY` et `ZZ` sont des numéros hexadécimaux valides entre 00 et FF. La valeur pour `XX` ne doit pas être supérieure à 3F afin d'éviter tout conflit avec des adresses MAC générées par VMware Workstation et les produits VMware Server. La valeur maximum pour une adresse MAC générée manuellement est la suivante :

```
ethernet<number>.address = 00:50:56:3F:FF:FF
```

Vous devez également configurer l'option dans le fichier de configuration d'une machine virtuelle :

```
ethernet<number>.addressType="static"
```

Étant donné que les machines virtuelles ESX de VMware ne prennent pas en charge les adresses MAC arbitraires, vous devez utiliser le format ci-dessus. Tant que vous choisissez une valeur unique pour `XX:YY:ZZ` parmi vos adresses codées de manière irréversible, les conflits entre les adresses MAC assignées automatiquement et manuellement ne devraient jamais se produire.

Génération d'adresses MAC

Chaque carte réseau virtuelle dans une machine virtuelle se voit attribuer une adresse MAC unique. Chaque fabricant de carte réseau se voit attribuer un préfixe unique à trois octets appelé OUI (Organizationally Unique Identifier) qu'il peut utiliser pour générer des adresses MAC uniques.

VMware possède les OUI suivants :

- Adresses MAC générées
- Adresses MAC configurées manuellement
- Pour les machines virtuelles héritées qui ne sont plus utilisées avec ESX

Les trois premiers octets de l'adresse MAC générée pour chaque carte réseau virtuelle correspondent au OUI. L'algorithme de génération d'adresse MAC produit les trois autres octets. L'algorithme garantit des adresses MAC uniques au sein d'une machine et tente de fournir des adresses MAC uniques à travers les machines.

Les cartes réseau pour chaque machine virtuelle du même sous-réseau doivent disposer d'adresses MAC uniques. Sinon, leur comportement risque d'être imprévisible. L'algorithme limite le nombre de machines virtuelles en exécution et suspendues, en même temps, sur un hôte donné. Il ne gère pas non plus tous les cas où des machines virtuelles sur des machines physiques distinctes partagent un sous-réseau.

L'identificateur unique universel VMware (UUID) génère des adresses MAC contrôlées pour les conflits. Les adresses MAC générées comportent trois parties : l'OUI VMware, l'UUID SMBIOS pour la machine physique ESX, et un hachage basé sur le nom de l'entité pour laquelle l'adresse MAC est générée.

Lorsque l'adresse MAC a été générée, elle ne change pas à moins que la machine virtuelle ne soit transférée à un emplacement différent (par exemple, un chemin d'accès différent sur le même serveur). L'adresse MAC dans le fichier de configuration de la machine virtuelle est enregistrée. Toutes les adresses MAC attribuées aux cartes réseau de machines virtuelles suspendues ou en exécution sur une machine physique donnée sont suivies.

L'adresse MAC d'une machine virtuelle hors tension n'est pas comparée aux adresses MAC de machines virtuelles suspendues ou en exécution. Lorsqu'une machine virtuelle est de nouveau mise sous tension, il se peut qu'elle acquière une adresse MAC différente. Cette acquisition est due à un conflit avec une machine virtuelle qui était sous tension quand cette machine virtuelle était hors tension.

Configurer une adresse MAC

Vous pouvez assigner des adresses MAC statiques aux NIC virtuels d'une machine virtuelle éteinte.

Procédure

1 Ouvrez une session sur le vSphere Client et sélectionnez la machine virtuelle dans le panneau d'inventaire.

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

3 Sélectionnez la carte réseau dans la liste Matériel.

4 Dans un groupes d'adresses MAC, sélectionnez **[Manuel]** .

5 Saisissez l'adresse MAC statique, puis cliquez sur **[OK]** .

Délestage de segmentation TCP et Trames jumbo

Vous devez activer des trames jumbo au niveau de l'hôte à l'aide de l'interface de ligne de commande afin de configurer la taille de MTU pour chaque commutateur vSwitch. Le délestage de segmentation TCP (TSO) est activé par défaut sur l'interface VMkernel, mais doit être activé au niveau de la machine virtuelle.

Activation du TSO (délestage de segmentation TCP)

Pour activer le TSO au niveau de la machine virtuelle, vous devez remplacer les cartes réseau virtuelles flexibles ou vmxnet existantes par des cartes réseau virtuelles vmxnet. Ce remplacement peut entraîner un changement d'adresse MAC de la carte réseau virtuelle.

Le support TSO via la carte réseau vmxnet amélioré est disponible pour les machines virtuelles exécutant les systèmes d'exploitation invités suivants :

- Microsoft Windows 2003 Enterprise Edition avec Service Pack 2 (32 bits et 64 bits)
- Red Hat Enterprise Linux 4 (64 bits)
- Red Hat Enterprise Linux 5 (32 bits et 64 bits)
- SUSE Linux Enterprise Server 10 (32 bits et 64 bits)

Activer le support TSO pour une machine virtuelle

L'activation du support TSO sur une machine virtuelle requiert un adapteur vmxnet amélioré

Procédure

1 Ouvrez une session sur le vSphere Client et sélectionnez la machine virtuelle dans le panneau d'inventaire.

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

3 Sélectionnez la carte réseau dans la liste Matériel.

4 Enregistrez les paramètres réseau et l'adresse MAC utilisés par la carte réseau.

5 Cliquez sur **[Supprimer]** pour supprimer la carte réseau de la machine virtuelle.

6 Cliquez sur **[Ajouter]** .

7 Sélectionnez **[Adaptateur Ethernet]** et cliquez sur **[Suivant]** .

8 Dans le groupes Types d'adaptateur, sélectionnez **[VMXNET 2 amélioré]** .

9 Sélectionnez le paramètre réseau et l'adresse MAC utilisés par l'ancienne carte réseau, puis cliquez sur **[Suivant]** .

10 Cliquez sur **[Terminer]** , puis sur **[OK]** .

11 Si la machine virtuelle n'est pas configurée pour mettre VMware Tools à niveau à chaque mise sous tension, vous devez le mettre manuellement à niveau.

TSO est activé sur une interface VMkernel. Si le TSO est désactivé pour une interface VMkernel spécifique, le seul moyen de l'activer est de supprimer cette interface VMkernel et de la recréer avec un TSO activé.

Contrôler l'activation du TSO sur une interface VMkernel

Vous pouvez contrôler l'activation du TSO sur une interface de réseau VMkernel spécifique.

Procédure

1 Ouvrez une session sur votre console d'hôte ESX.

2 Utilisez la commande **`esxcfg-vmknic -l`** pour afficher une liste d'interface VMkernel.

La liste indique chaque interface VMkernel disposant d'une activation TSO, avec TSO MSS défini sur 65535.

Suivant

Si le TSO n'est pas activé pour une interface VMkernel spécifique, le seul moyen de l'activer est de supprimer l'interface VMkernel et de la recréer.

Activation de Trames jumbo

Les Trames jumbo permettent à ESX d'envoyer des trames plus grandes sur le réseau physique. Le réseau doit prendre en charge des Trames jumbo de bout en bout.

Les Trames jumbo jusqu'à 9 Ko (9000 octets) sont prises en charge.

Les Trames jumbo doivent être activées pour chaque interface VMkernel ou commutateur vSwith via l'interface de ligne de commande sur votre hôte ESX. Avant d'activer des trames jumbo, consultez votre fournisseur de matériel afin de garantir que votre carte réseau physique prenne en charge les trames jumbo.

Créer un commutateur vSwitch avec Trames jumbo activé

Vous pouvez configurer un commutateur vSwitch pour des trames Jumbo en modifiant la taille de MTU pour chaque vSwitch.

Procédure

1 Utilisez la commande **`vicfg-vswitch -m <MTU> <vSwitch>`** dans l'interface de ligne de commande vSphere de VMware afin de régler la taille de MTU du vSwitch.

Cette commande configure le MTU pour toutes les liaisons montantes sur chaque vSwitch. Configurez la taille de MTU sur le paramètre le plus élevé parmi toutes les cartes réseau virtuelles reliées au vSwitch.

2 Utilisez la commande **`vicfg-vswitch -l`** pour afficher une liste de commutateurs vSwitch sur l'hôte et vérifier que la configuration du vSwitch est correcte.

Activer Trames jumbo sur un commutateur distribué vNetwork

Vous activez un commutateur distribué vNetwork pour trames Jumbo en modifiant la taille de MTU pour ce commutateur.

Procédure

1 Dans vSphere Client, affichez la vue d'inventaire de mise en réseau et sélectionnez le commutateur distribué vNetwork.

2 Dans le menu Inventaire, sélectionnez **[Commutateur distribué vNetwork] > [Modifier les paramètres]** .

3 Sur l'onglet **[Propriétés]** , sélectionnez **[Avancé]** .

4 Configurez **[MTU max.]** sur la taille de MTU maximale parmi toutes les cartes réseau virtuelles reliées au commutateur distribué vNetwork, puis cliquez sur **[OK]** .

Activer la prise en charge de Trames jumbo sur une machine virtuelle

L'activation de la prise en charge de trames Jumbo sur une machine virtuelle requiert un adapteur vmxnet amélioré.

Procédure

1 Ouvrez une session sur le vSphere Client et sélectionnez la machine virtuelle dans le panneau d'inventaire.

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

3 Sélectionnez la carte réseau dans la liste Matériel.

4 Enregistrez les paramètres réseau et l'adresse MAC utilisés par la carte réseau.

5 Cliquez sur **[Supprimer]** pour supprimer la carte réseau de la machine virtuelle.

6 Cliquez sur **[Ajouter]** .

7 Sélectionnez **[Adaptateur Ethernet]** et cliquez sur **[Suivant]** .

8 Dans le groupes Type d'adaptateur, sélectionnez **[VMXNET 2 amélioré]** .

9 Sélectionnez le réseau utilisé par l'ancienne carte réseau, puis cliquez sur **[Suivant]** .

10 Cliquez sur **[Terminer]** .

11 Sélectionnez le nouvel adaptateur réseau dans la liste Matériel.

12 Sous Adresse MAC, sélectionnez **[Manuel]** , puis saisissez l'adresse MAC utilisée par l'ancienne carte réseau.

13 Cliquez sur **[OK]** .

14 Vérifiez que la carte vmxnet amélioré est reliée à un commutateur vSwitch avec trames Jumbo activées.

15 Dans le système d'exploitation invité, configurez la carte réseau de manière à autoriser les trames Jumbo.

Consultez la documentation du système d'exploitation invité pour plus de détails.

16 Configurez tous les commutateurs physiques et les machines virtuelles ou physiques auxquelles cette machine virtuelle se connecte pour prendre en charge les trames Jumbo.

Créer une interface VMkernel avec Trames jumbo activé

Vous pouvez créer une interface réseau VMkernel activée avec Trames jumbo.

Procédure

1 Ouvrez une session sur votre console d'hôte ESX.

2 Utilisez la commande **esxcfg-vmknic -a -I <ip address> -n <netmask> -m <MTU> <port group name>** pour créer une connexion VMkernel avec un support Trames jumbo.

3 Utilisez la commande **esxcfg-vmknic -l** pour afficher une liste d'interfaces VMkernel et vérifier que la configuration de l'interface avec Trames jumbo est correcte.

4 Vérifiez que l'interface VMkernel est connectée à un commutateur vSwitch avec Trames jumbo activé.

5 Configurez tous les commutateurs physiques et les machines virtuelles ou physiques auxquelles cette interface VMkernel se connecte pour prendre en charge les Trames jumbo.

NetQueue et performances réseau

NetQueue dans ESX tire profit de la capacité de certaines cartes réseau à fournir au système un trafic réseau dans plusieurs files d'attente de réception pouvant être traitées séparément, ce qui permet un fonctionnement à l'échelle de plusieurs CPU et une augmentation significative des performances réseau.

Activer NetQueue sur un hôte ESX

NetQueue est activé par défaut. Pour pouvoir utiliser NetQueue, vous devez le réactiver s'il a été désactivé.

Prérequis

Familiarisez-vous avec les informations de configuration des pilotes NIC du *Guide de référence d'installation de VMware vSphere Command-Line Interface*.

Procédure

1 Dans le VMware vSphere CLI, utilisez la commande `vicfg-advcfg --set true VMkernel.Boot.netNetQueueEnable`.

2 Utilisez l'interface de ligne de commande vSphere de VMware afin de configurer le pilote NIC pour pouvoir utiliser NetQueue.

3 Redémarrez l'hôte ESX.

Désactiver NetQueue sur un hôte ESX

NetQueue est activé par défaut.

Procédure

1 Dans le VMware vSphere CLI, utilisez la commande `vicfg-advcfg --set false VMkernel.Boot.netNetQueueEnable`.

2 Pour désactiver NetQueue sur le pilote NIC, utilisez la commande `vicfg-module -s "" module name`.

Par exemple, si vous servez du pilote s2io NIC, utilisez `vicfg-module -s "" s2io`.

3 Redémarrez l'hôte.

E/S VMDirectPath

E/S VMDirectPath permet à une machine virtuelle d'accéder aux fonctions physiques PCI sur les plates-formes avec une unité de gestion de mémoire E/S.

Les fonctionnalités suivantes ne sont pas disponibles pour les machines virtuelles configurées avec VMDirectPath :

- vMotion
- Retrait ou ajout à chaud de périphériques virtuels
- Interruption et reprise
- Enregistrement et lecture
- Tolérance aux pannes
- Haute disponibilité
- DRS (disponibilité limitée. La machine virtuelle peut faire partie d'un cluster, mais pas migrer à travers des hôtes)

Voir les guides de compatibilité matérielle pour les derniers systèmes et adaptateurs pris en charge avec cette configuration.

Configurer les périphériques de relais sur un hôte

Vous pouvez configurer des périphériques réseau de relais sur un hôte.

Procédure

1 Sélectionnez un hôte dans le panneau d'inventaire de vSphere Client.

2 Dans l'onglet **[Configuration]** , cliquez sur **[Paramètres avancés]** .

La page Passthrough Configuration apparaît, énumérant tous les périphériques de relais disponibles. Une icône verte indique qu'un périphérique est activé et actif. Une icône orange indique que l'état du périphérique a changé et l'hôte doit être redémarré avant que le périphérique puisse être utilisé.

3 Cliquez sur **[Modifier]** .

4 Sélectionnez les périphériques à utiliser pour le relais et cliquez sur **[OK]** .

Configurer un périphérique PCI sur une machine virtuelle

Vous pouvez configurer un périphérique PCI de relais sur une machine virtuelle.

Procédure

1 Sélectionnez une machine virtuelle dans le panneau de l'inventaire du vSphere Client.

2 Dans le menu **[inventaire]** , sélectionnez **[Machine virtuelle] > [Modifier les paramètres]** .

3 Sous l'onglet **[Matériel]** , cliquez sur **[Ajouter]** .

4 Sélectionnez **[Périphérique PCI]** et cliquez sur **[Suivant]** .

5 Sélectionnez le périphérique de relais à utiliser, et cliquez sur **[Suivant]** .

6 Cliquez sur **[Terminer]** .

Ajouter un périphérique VMDirectPath à une machine virtuelle configure la réservation de mémoire sur la taille de mémoire de la machine virtuelle.

Meilleures pratiques, scénarios et dépannage du réseau 6

Les meilleures pratiques, scénarios de configuration et recommandations de dépannage suivants fournissent des suggestions pour les configurations réseau et erreurs antipattern communes.

Ce chapitre aborde les rubriques suivantes :

Meilleures pratiques de mise en réseau

Prenez en compte ces meilleures pratiques pour la configuration de votre réseau.

- Séparez les services réseau les uns des autres pour obtenir une sécurité accrue ou de meilleures performances.

  Pour qu'un ensemble particulier de machines virtuelles fonctionne aux niveaux les plus élevés de performances, placez-les sur un NIC physique séparé. Cette séparation permet de répartir plus équitablement sur plusieurs CPU une partie de la charge de travail totale du réseau. Les machines virtuelles isolées peuvent ensuite mieux servir le trafic à partir d'un client Web, par exemple.

- Vous pouvez respecter les recommandations suivantes soit en utilisant le VLAN pour segmenter un réseau physique unique, soit en séparant des réseaux physiques (la dernière option est préférable).

  - Conserver la console du service sur son propre réseau est une partie importante de la sécurisation du système ESX. Prenez en compte la connectivité du réseau de la console du service tout comme n'importe quel périphérique d'accès à distance dans un hôte, car compromettre la console du service donne le contrôle total à un attaquant sur toutes les machines virtuelles s'exécutant sur le système.

  - Conserver la connexion vMotion sur un réseau séparé dédié à vMotion est important, car le contenu de la mémoire du système d'exploitation invité est transmis sur le réseau au cours de la migration vMotion.

- Lors de l'utilisation de périphériques de relais avec un noyau Linux version 2.6.20 ou antérieure, évitez les modes MSI et MSI-X, car ces modes ont un impact important sur les performances.

- Pour séparer physiquement des services réseau et dédier un ensemble particulier de NIC à un service réseau spécifique, créez un vSwitch pour chaque service. Si cela est impossible, séparez-les sur un seul vSwitch en les associant aux groupes de ports avec différents ID de VLAN. Dans ce cas, vérifiez auprès de votre administrateur réseau que les réseaux ou VLAN que vous choisissez sont isolés dans le reste de votre environnement et qu'aucun routeur ne les connecte.

- Vous pouvez ajouter et supprimer des NIC du vSwitch sans affecter les machines virtuelles ou le service réseau s'exécutant derrière ce vSwitch. Si vous supprimez tout le matériel en cours d'exécution, les machines virtuelles peuvent toujours communiquer entre elles. Par ailleurs, si vous laissez un NIC intact, toutes les machines virtuelles peuvent toujours se connecter au réseau physique.
- Pour protéger vos machines virtuelles les plus sensibles, déployez des pare-feu dans les machines virtuelles qui acheminent du trafic entre les réseaux virtuels avec des liaisons montantes vers des réseaux physiques et les réseaux virtuels purs sans liaisons montantes.

Montage de volumes NFS

Dans ESX, le modèle montrant comment ESX accède au stockage NFS des images ISO utilisées comme CD-ROM virtuels pour les machines virtuelles est différent du modèle utilisé dans ESX Server 2.x.

ESX prend en charge les montages NFS basés sur VMkernel. Le nouveau modèle consiste à monter votre volume NFS avec les images ISO grâce à la fonctionnalité NFS de VMkernel. Tous les volumes NFS montés de cette manière apparaissent sous forme de banque de données dans vSphere Client. L'éditeur de configuration de machine virtuelle vous permet de parcourir le système de fichiers de la console du service pour rechercher les images ISO à utiliser comme périphériques CD-ROM virtuels.

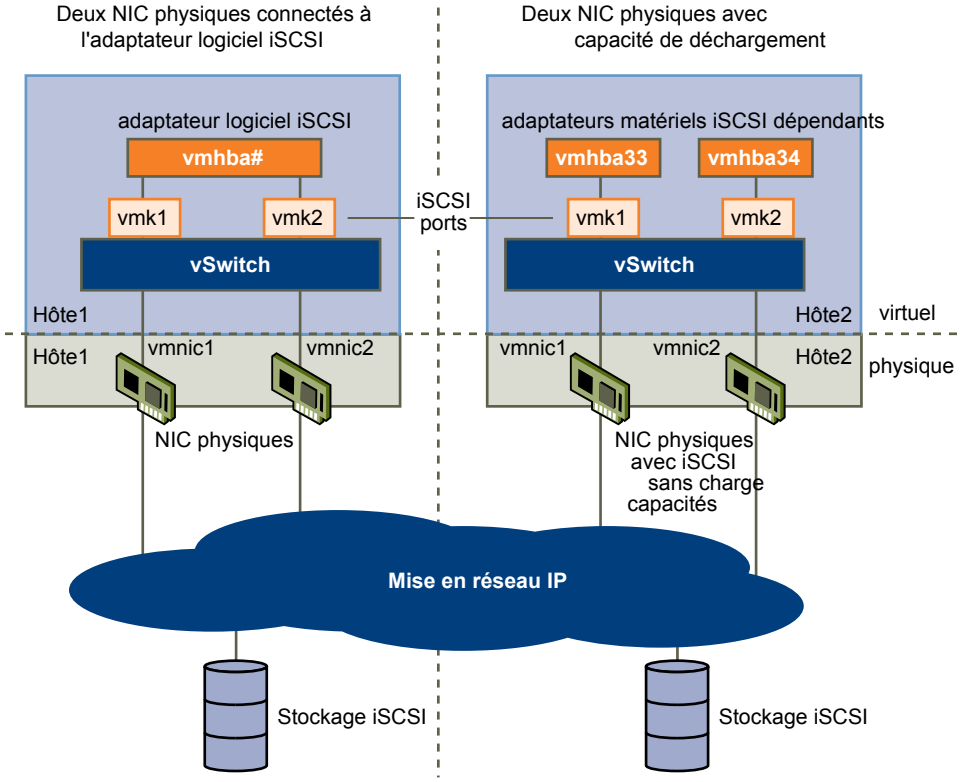
Configuration du réseau pour l'iSCSI logiciel et l'iSCSI matériel dépendant

Si vous utilisez l'adaptateur iSCSI logiciel ou les adaptateurs iSCSI matériels dépendants, vous devez configurer le réseau pour l'iSCSI pour pouvoir activer et configurer vos adaptateurs iSCSI. La configuration du réseau pour le iSCSI implique d'ouvrir un port iSCSI VMkernel pour le trafic entre l'adaptateur iSCSI et le NIC physique.

Selon le nombre de NIC physiques utilisés par votre trafic iSCSI, la configuration réseau peut varier.

- Si vous n'avez qu'un seul NIC physique, créez un port iSCSI sur un vSwitch connecté au NIC. VMware vous recommande de désigner un adaptateur réseau séparé pour le iSCSI. N'utilisez pas d'iSCSI sur des adaptateurs 100Mbps ou plus lents.
- Si vous disposez de deux ou plus NIC physiques pour le iSCSI, créez un port iSCSI distinct pour chaque NIC physique et utilisez les NICs pour un multichemin iSCSI. Reportez-vous à Figure 6-1.

Figure 6-1. Mise en réseau avec iSCSI



Remarque Lorsque vous utilisez un adaptateur iSCSI matériel dépendant, le rapport de performances pour un NIC associé à l'adaptateur ne ne montre que peu ou pas d'activité, même lorsque le trafic iSCSI est intense. Cela est du au contournement de la pile réseau habituelle par le trafic iSCSI.

Créer un port iSCSI pour un NIC unique

Utilisez cette tâche pour connecter le VMkernel, qui exécute les services pour le stockage iSCSI, à une carte réseau physique. Si vous n'avez qu'une seule carte réseau physique exploitable pour le trafic iSCSI, voici la seule procédure à suivre pour configurer votre réseau iSCSI.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Mise en réseau]** .

3 Dans la vue commutateur virtuel, cliquez sur **[Ajouter gestion réseau]** .

4 Sélectionnez **[VMkernel]** et cliquez sur **[Suivant]** .

5 Sélectionnez **[Créer un commutateur virtuel]** pour créer un nouveau vSwitch.

6 Sélectionnez le NIC que vous voulez utiliser pour le trafic iSCSI.

IMPORTANT Si vous créez un port pour l'adaptateur matériel dépendant iSCSI, assurez-vous de choisir le NIC qui correspond au composant iSCSI. Reportez-vous à « Détermine l'association entre les adaptateurs de matériel iSCSI dépendants et les adaptateurs réseau physiques », page 106.

7 Cliquez sur **[Suivant]** .

8 Entrez une étiquette de réseau.

L'étiquette de réseau est un nom facilement mémorisable qui identifie le port VMkernel que vous venez de créez, par exemple iSCSI.

9 Cliquez sur **[Suivant]** .

10 Configurez l'IP puis cliquez sur **[Suivant]** .

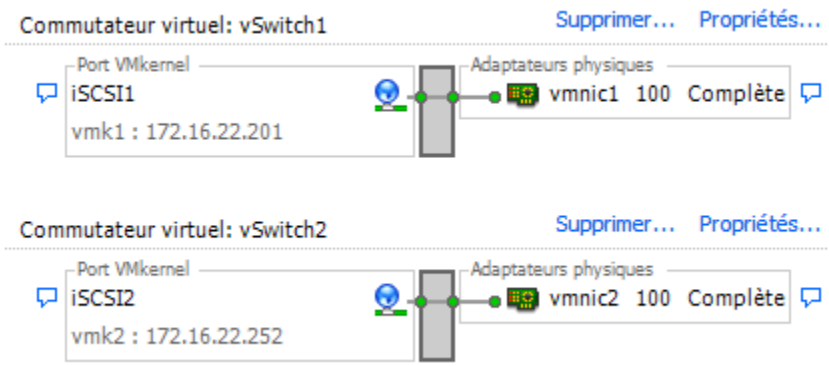
11 Passez vos informations en revue et cliquez sur **[Terminer]** .

Utilisation de plusieurs NIC pour l'iSCSI logiciel et l'iSCSI matériel dépendant

Si votre hôte possède plusieurs adaptateurs réseau physiques pour l'iSCSI, créez un port iSCSI distinct pour chaque carte physique avec un mappage 1:1.

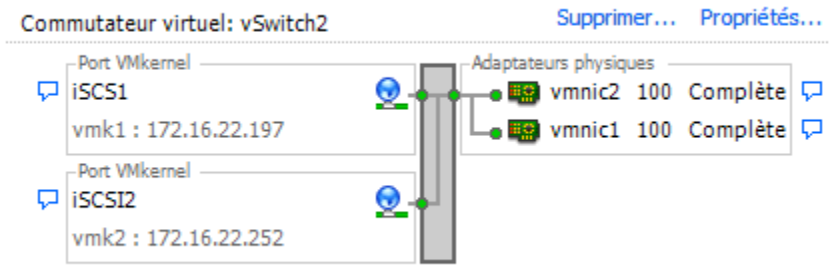
Pour réaliser le mappage 1:1, désignez un vSwitch distinct pour chaque adaptateur réseau et paire de ports iSCSI. Reportez-vous à Figure 6-2.

Figure 6-2. Ports iSCSI et NIC sur vSwitch distincts



Il est également possible d'ajouter tous les NIC et paires de ports à un unique vSwitch. Reportez-vous à Figure 6-3. Vous devez modifier le réglage par défaut et vérifier que chaque port soit mappé avec un seul NIC actif correspondant.

Figure 6-3. Ports iSCSI et NIC sur vSwitch unique



Pour en savoir plus sur l'ajout de NIC et de paires de ports VMkernel à un vSwitch, reportez-vous à la section « Créer des ports iSCSI supplémentaires pour NIC multiples », page 77.

Après avoir mappé les ports iSCSI sur les adaptateurs réseau, utilisez la commande `esxcli` pour associer les ports aux adaptateurs iSCSI. Associez les ports avec les adaptateurs iSCSI matériels dépendants, que vous utilisiez un seul ou de multiples NIC. Pour plus d'informations, consultez « Associer des ports iSCSI aux adaptateurs iSCSI », page 107.

Créer des ports iSCSI supplémentaires pour NIC multiples

Utilisez cette tâche si vous dispsez de deux cartes réseau ou plus que vous pouvez assigner au iSCSI et si vous voulez connecter toutes vos cartes réseau iSCSI à un vSwitch unique. Cette tâche vous permet d'associer des ports iSCSI VMkernel aux adaptateurs réseau grâce à un mappage 1:1.

Vous devez à présent connecter les NIC supplémentaires au vSwitch existant et les mapper vers les ports iSCSI correspondants.

Remarque Si vous utilisez un commutateur distribué par vNetwork avec dvUplinks multiples, pour l'association de ports créez un groupes dvPort distinct pour chaque NIC physique. Puis réglez la politique de groupes de façon à ce que chaque dvPort n'ait qu'un seul dvUplink actif.

Pour des informations plus détaillées sur les commutateurs distribués par vNetwork, consultez la section Mise en réseau.

Prérequis

Vous devez créer un vSwitch qui mappe un port iSCSI vers un NIC physique désigné pour le trafic iSCSI.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Mise en réseau]** .

3 Sélectionnez le vSwitch que vous voulez utiliser pour le iSCSI et cliquez sur **[Propriétés]** .

4 Connectez des adaptateurs réseau supplémentaires au vSwitch.

   a Dans la boîte de dialogue Propriétés vSwicth, sélectionnez l'onglet **[Adaptateurs réseau]** puis cliquez sur **[Ajouter]** .

   b Sélectionnez un NIC ou plus dans la liste puis cliquez sur **[Suivant]** .

   En cas d'adaptateurs iSCSI matériels dépendants, assurez-vous de choisir seulement les NIC ayant un composant iSCSI correspondant.

   c Passez en revue les informations sur la page Résumé d'adaptateur, puis cliquez sur **[Terminer]** .

   La liste des adaptateurs réseau réapparaît, montrant les adaptateurs réseau maintenant revendiqués par le vSwitch.

5 Créez des ports iSCSI pour tous les NIC que vous avez connectés.

   Le nombre de ports iSCSI doit correspondre au nombre de NIC dans le vSwitch.

   a Dans la boîte de dialogue Propriétés vSwicth, sélectionnez l'onglet **[Ports]** puis cliquez sur **[Ajouter]** .

   b Sélectionnez **[VMkernel]** et cliquez sur **[Suivant]** .

   c Sous **[Propriétés groupe de ports]** , entrez une étiquette de réseau, par exemple iSCSI, puis cliquez sur **[Suivant]** .

   d Configurez l'IP puis cliquez sur **[Suivant]** .

   Lorsque vous entrez un masque de sous-réseau, assurez-vous que le NIC est réglé sur le sous-réseau du système de stockage auquel il se connecte.

   e Passez vos informations en revue et cliquez sur **[Terminer]** .

AVERTISSEMENT Si le NIC que vous utilisez avec votre adaptateur iSCSI, qu'il soit logiciel ou matériel dépendant, ne se trouve pas dans le même sous-réseau que votre cible iSCSI, votre hôte ne pourra pas établir de sessions de cet adaptateur réseau vers la cible.

6 Mappez chaque port iSCSI sur un seul NIC actif.

   Par défaut, pour chaque port iSCSI sur le vSwitch, tous les adaptateurs réseau sont affichés comme actifs. Vous devez ignorer ce réglage par défaut pour que chaque port soit mappé vers un seul NIC actif correspondant. Par exemple, le port iSCSI vmk1 est mappé sur vmnic1, le port vmk2 est mappé sur vmnic2, etc.

   a Dans l'onglet **[Ports]** , sélectionnez un port iSCSI et cliquez sur **[Modifier]** .

   b Cliquez sur l'onglet **[Association de cartes réseau]** puis sélectionnez **[Remplacer la commande de basculement vSwitch]** .

   c Désignez un seul adaptateur comme actif et déplacez tout le reste vers la catégorie **[Adaptateurs inutilisés]** .

7 Répétez cette dernière étape pour chaque port iSCSI sur le vSwitch.

Suivant

Une fois cette tâche terminée, lancez la commande `esxcli` pour associer les ports iSCSI aux adaptateurs iSCSI logiciels ou matériels dépendants.

Configuration du réseau sur des serveurs lame

Comme les serveurs lame ont un nombre limité d'adaptateurs réseau, vous pouvez utiliser les VLAN pour séparer le trafic de la console du service, de vMotion, du stockage IP et de divers groupes de machines virtuelles.

Les meilleures pratiques de VMware recommandent que la console du service et vMotion aient leurs propres réseaux pour des raisons de sécurité. Si vous dédiez des adaptateurs physiques à des vSwitch séparés dans cet objectif, vous pouvez éliminer les connexions redondantes (associées), arrêter d'isoler les différents clients réseau, ou les deux. Les VLAN vous permettent d'atteindre une segmentation du réseau sans devoir utiliser plusieurs adaptateurs physiques.

Pour que la lame réseau d'un serveur lame prenne en charge le groupes de ports ESX avec le trafic balisé du VLAN, vous devez configurer la lame pour prendre en charge le protocole 802.1Q et configurer le port comme un port balisé.

La méthode de configuration d'un port comme un port balisé diffère d'un serveur à un autre. La liste décrit comment configurer un port balisé sur trois des serveurs lame les plus utilisés.

Tableau 6-1. Options de balisage des ports sur des serveurs lame

Type de serveur	Option de configuration
HP Blade	Définissez **[Marquage VLAN]** sur **[Activé]** .
Dell PowerEdge	Définissez le port sur **[Marqué]** .
IBM eServer Blade Center	Sélectionnez **[Balise]** dans la configuration du port.

Configuration d'un groupes de ports de machine virtuelle avec un VLAN sur un serveur lame

La configuration du réseau de machines virtuelles sur un serveur lame nécessite certaines considérations spéciales.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** , puis sur **[Mise en réseau]** .

3 Sur le côté droit de la page, cliquez sur **[Propriétés]** pour le vSwitch associé à la console du service.

4 Sous l'onglet **[Ports]** , cliquez sur **[Ajouter]** .

5 Sélectionnez **[Machines virtuelles]** pour le type de connexion (valeur par défaut).

6 Cliquez sur **[Suivant]** .

7 Dans le groupes Propriétés groupes de ports, entrez une étiquette de réseau qui identifie le groupes de ports que vous créez.

   Utilisez des étiquettes réseau pour identifier les connexions compatibles pour la migration communes à deux hôtes ou plus.

8 Dans le champ **[ID VLAN]** , entrez un nombre entre 1 et 4 094.

   Si vous n'êtes pas sûr de la valeur qu'il faut entrer, laissez ce champ vide et demandez à votre administrateur réseau.

9 Cliquez sur **[Suivant]** .

10 Après avoir déterminé que le vSwitch est configuré correctement, cliquez sur **[Terminer]** .

Configuration d'un port VMkernel avec un VLAN sur un serveur lame

Vous pouvez configurer une interface réseau VMkernel à l'aide d'un VLAN sur un serveur lame.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** , puis sur **[Mise en réseau]** .

3 Sur le côté droit de la page, cliquez sur **[Propriétés]** pour le vSwitch associé à la console du service.

4 Sous l'onglet **[Ports]** , cliquez sur **[Ajouter]** .

5 Sélectionnez **[VMkernel]** et cliquez sur **[Suivant]** .

Cette option vous permet de connecter le réseau physique à VMkernel, qui exécute les services pour vMotion et le stockage IP (NFS ou iSCSI).

6 Dans le groupes Propriétés groupes de ports, sélectionnez ou entrez l'étiquette de réseau et un ID de VLAN.

Entrez une étiquette de réseau pour identifier le groupes de ports que vous créez. Il s'agit de l'étiquette que vous définissez lors de la configuration d'un adaptateur virtuel à associer à ce groupes de ports, lors de la configuration des services VMkernel, tels que vMotion et le stockage IP.

Entrez un ID de VLAN pour identifier le VLAN que le trafic réseau du groupes de ports utilisera.

7 Sélectionnez **[Utiliser ce groupes port pour vMotion]** pour permettre à ce groupes de ports de s'annoncer à un autre hôte ESX comme connexion réseau où le trafic de vMotion doit être envoyé.

Vous pouvez activer cette propriété pour un seul groupes de ports vMotion et de stockage IP pour chaque hôte ESX. Si cette propriété n'est pas activée pour un groupes de ports, la migration avec vMotion vers cet hôte n'est pas possible.

8 Dans le groupes paramètre d'IP, cliquez sur **[Modifier]** pour définir la passerelle VMkernel par défaut pour les services VMkernel, tels que vMotion, NAS et iSCSI.

Dans l'onglet **[Config. DNS]** , le nom de l'hôte est entré dans le champ nom par défaut. Les adresses de serveur DNS et le domaine spécifiés pendant l'installation sont également présélectionnée.

Dans l'onglet **[Routage]** , la console du service et VMkernel ont chacun besoin de leurs propres informations de passerelle. Une passerelle est nécessaire pour une connectivité aux ordinateurs qui ne résident pas sur le même sous-réseau IP que la console de service ou VMkernel.

Les paramètres IP sont statiques par défaut.

9 Cliquez sur **[OK]** , puis sur **[Suivant]** .

10 Cliquez sur **[Retour]** pour apporter des modifications.

11 Vérifiez vos modifications sur la page Prêt à terminer et cliquez sur **[Terminer]** .

Dépannage

Vous devriez rencontrer des problèmes de réseau hôte nécessitant un dépannage. Dans la plupart des cas, le réseau hôte peut être restauré avec quelques changements de configuration.

Dépannage de la mise en réseau de la console du service

Si certaines parties du réseau de la console du service sont mal configurées, vous ne pouvez pas accéder à votre hôte ESX avec vSphere Client.

Si la console du service de votre hôte perd la connectivité réseau, vous pouvez reconfigurer le réseau en vous connectant directement à la console du service et en utilisant les commandes de cette console.

- `esxcfg-vswif -l`

  Fournit une liste des interfaces réseau actuelles de la console du service. Vérifiez que `vswif0` est présent et que l'adresse IP courante et le masque de réseau sont corrects.

- `esxcfg-vswitch -l`

  Fournit une liste des configurations de commutateur virtuel courant. Vérifiez que l'adaptateur de liaison montante configuré pour la console du service est connecté au réseau physique approprié.

- `exscfg-nics -l`

  Fournit une liste des adaptateurs réseau courants. Vérifiez que l'adaptateur de liaison montante configuré pour la console du service est en fonctionnement et que la vitesse et le duplex sont tous deux corrects.

- `esxcfg-nics -s <vitesse> <nic>`

  Modifie la vitesse de l'adaptateur réseau.

- `esxcfg-nics -d <duplex> <nic>`

  Modifie le duplex de l'adaptateur réseau.

- `esxcfg-vswif -I <nouvelle adresse ip> vswifX`

  Modifie l'adresse IP de la console du service.

- `esxcfg-vswif -n <nouveau masque réseau> vswifX`

  Modifie le masque réseau de la console du service.

- `esxcfg-vswitch -U <ancien vmnic> <service de console vswitch>`

  Supprime la liaison montante de la console du service.

- `esxcfg-vswitch -L <nouveau vmnic> <service de console vswitch>`

  Modifie la liaison montante de la console du service.

Si vous rencontrez une longue attente lorsque vous utilisez les commandes `esxcfg-*`, le DNS est peut-être mal configuré. Les commandes `esxcfg-*` nécessitent que le DNS soit reconfiguré afin que la résolution de nom localhost fonctionne correctement. Cela nécessite que le fichier `/etc/hosts` contienne une entrée pour l'adresse IP configurée et l'adresse localhost 127.0.0.1 localhost.

Changement de nom des adaptateurs réseau à l'aide de la console du service

Si vous perdez la connectivité à la console du service après l'ajout d'un nouvel adaptateur réseau, vous devez utiliser la console du service pour renommer les adaptateurs réseau concernés. L'ajout d'un nouvel adaptateur réseau peut provoquer la perte de connectivité à la console du service et d'administration de cette dernière à l'aide de vSphere Client en raison du changement de nom des adaptateurs réseau.

Procédure

1 Connectez-vous directement à la console de l'hôte ESX.

2 Utilisez la commande `esxcfg-nics -l` pour voir les noms ayant été attribués aux adaptateurs réseau.

3 Utilisez la commande `esxcfg-vswitch -l` pour voir les vSwitch maintenant associés à des noms de périphériques qui ne sont plus visibles dans `esxcfg-nics`.

4 Utilisez la commande `esxcfg-vswitch -U <ancien nom vmnic> <vswitch>` pour supprimer les adaptateurs réseau qui ont été renommés.

5 Utilisez la commande `esxcfg-vswitch -L <nouveau nom vmnic> <vswitch>` pour ajouter les adaptateurs réseau à nouveau en leur donnant des noms corrects.

Dépannage de la configuration d'un commutateur physique

La connectivité de commutateur vSwitch peut être perdue en cas d'événement de basculement ou de retour arrière. Cela fait que les adresses MAC que les machines virtuelles ont associées à ce vSwitch semblent se trouver sur un port de commutateur différent.

Pour éviter ce problème, placez votre commutateur physique en mode Portfast ou joncteur PortFast.

Dépannage de la configuration du groupes de ports

La modification du nom d'un groupes de ports lorsque des machines virtuelles sont déjà connectées à ce groupes de ports provoque une configuration réseau non valide des machines virtuelles configurées pour se connecter à ce groupes de ports.

La connexion à partir des adaptateurs réseau virtuels aux groupes de ports est effectuée par nom, et le nom est l'identifiant qui est stocké dans la configuration de la machine virtuelle. La modification du nom d'un groupes de ports ne provoque pas une reconfiguration massive de toutes les machines virtuelles connectées à ce groupes de ports. Les machines virtuelles déjà sous tension continuent à fonctionner jusqu'à ce qu'elles soient mises hors tension, car leurs connexions au réseau sont déjà établies.

Évitez de renommer les réseaux après qu'ils sont utilisés. Après avoir renommé un groupes de ports, vous devez reconfigurer chaque machine virtuelle associée en utilisant la console du service pour associer le nouveau nom du groupes de ports.

Stockage

Introduction au stockage 7

Cette introduction décrit les options de stockage disponibles pour ESX et explique comment configurer votre système ESX de sorte qu'il puisse utiliser et gérer différents types de stockage.

Ce chapitre aborde les rubriques suivantes :

À propos du stockage ESX

Le stockage ESX fait référence à l'espace de stockage sur divers systèmes de stockage physiques, locaux ou en réseau, qu'un hôte utilise pour stocker des disques de machines virtuelles.

Une machine virtuelle emploie un disque dur virtuel pour stocker son système d'exploitation, des fichiers de programme et d'autres données liées à ses activités. Un disque virtuel est un grand fichier physique, ou un ensemble de fichiers, qui peut être copié, déplacé, archivé et sauvegardé aussi facilement que n'importe quel autre fichier. Pour stocker des fichiers de disque virtuel et les manipuler, un hôte requiert un espace de stockage dédié.

L'hôte utilise l'espace de stockage sur divers systèmes de stockage physiques, y compris les périphériques externes et internes de votre hôte, ou un stockage en réseau, destiné aux tâches spécifiques de stockage et de protection des données.

Un hôte peut découvrir les périphériques de stockage auxquels il a accès et les formater en tant que banque de données. La banque de données est un conteneur logique spécial, analogue à un système de fichiers, où ESX place des fichiers du disque virtuel et d'autres fichiers qui encapsulent les éléments essentiels d'une machine virtuelle. Déployées sur différents périphériques de stockage, les banque de données masquent les informations de chaque périphérique de stockage et fournissent un modèle uniforme pour stocker des fichiers de machines virtuelles.

À l'aide du vSphere Client, vous pouvez configurer des banque de données sur un périphérique de stockage quelconque que votre hôte découvre. Vous pouvez également employer des dossiers pour créer des groupes logiques de banque de données à des fins organisationnelles et définir des autorisations et des alarmes dans le groupes de banque de données.

Types de stockage physique

Le processus de gestion de stockage ESX débute avec l'espace de stockage préalloué par votre administrateur stockage sur différents systèmes de stockage.

ESX prend en charge les types de stockage suivants :

Stockage local Stocke des fichiers de machine virtuelle sur des disques de stockage externes connectés directement ou internes.

Stockage en réseau Stocke des fichiers de machine virtuelle sur des baies ou disques de stockage externes reliés à votre hôte via une connexion directe ou un réseau haut débit.

Stockage local

Le stockage local peut être des disques durs internes situés dans votre hôte ESX, ou des systèmes de stockage externes situés à l'extérieur ou directement connectés à l'hôte via des protocoles comme SAS ou SATA.

Le stockage local ne requiert pas de réseau de stockage pour communiquer avec votre hôte. Vous avez besoin d'un câble connecté à l'unité de stockage et, si nécessaire, d'un HBA compatible dans votre hôte.

ESX prend en charge divers périphériques de stockage local internes et externes, y compris des systèmes de stockage SAS, SCSI, IDE, SATA et USB. Quel que soit le type de stockage utilisé, votre hôte masque une couche de stockage physique aux machines virtuelles.

Remarque Vous ne pouvez pas utiliser de lecteurs IDE/ATA pour stocker des machines virtuelles.

Les périphériques de stockage local ne prend en chargent pas le partage sur plusieurs hôtes. Une banque de données sur un périphérique de stockage local peut être accédée seulement par un seul hôte.

Puisque la majorité des périphériques de stockage local ne prennent pas en charge de connexions multiples, vous ne pouvez pas utiliser plusieurs chemins d'accès pour accéder au stockage local.

Stockage en réseau

Le stockage en réseau est composé de systèmes de stockage externes que votre hôte ESX utilise pour stocker des fichiers de machine virtuelle à distance. En règle générale, l'hôte accède à ces systèmes sur un réseau de stockage haut-débit.

Les périphériques de stockage en réseau sont partagés. Les banque de données sur des périphériques de stockage en réseau sont accessibles par plusieurs hôtes simultanément. ESX prend en charge les technologies de stockage en réseau suivantes.

Remarque L'accès simultané au même stockage via des protocoles de transport différents, tels qu'iSCSI et Fibre Channel, n'est pas pris en charge.

Fibre Channel (FC) Stocke des fichiers de machine virtuelle à distance sur un réseau de zone de stockage FC (SAN). FC SAN est un réseau haut débit spécialisé qui connecte vos hôtes à des périphériques de stockage haute performance. Le réseau utilise le protocole Fibre Channel pour acheminer le trafic SCSI depuis des machines virtuelles vers des périphériques FC SAN.

Pour se connecter au FC SAN, votre hôte doit être équipé d'adaptateurs de bus hôte (HBA) Fibre Channel. À moins d'utiliser un stockage de connexion directe Fibre Channel, vous avez besoin de commutateurs Fibre Channel pour acheminer le trafic de stockage. Si votre hôte contient des HBA FCoE (Fibre Channel over Ethernet), vous pouvez vous connecter à vos périphériques Fibre Channel partagés à l'aide d'un réseau IP.

SCSI Internet (iSCSI) Stocke des fichiers de machine virtuelle sur des périphériques de stockage iSCSI à distance. iSCSI rassemble le trafic de stockage SCSI dans le protocole TCP/IP de sorte qu'il puisse être acheminé via des réseaux TCP/IP standard, et non le réseau FC spécialisé. Grâce à une connexion iSCSI, votre hôte sert d'initiateur qui communique avec une cible, située dans des systèmes de stockage iSCSI à distance.

ESX offre les types de connexion iSCSI suivants :

iSCSI matérielle Votre hôte se connecte au stockage via un adaptateur tiers capable de décharger la gestion de réseau et iSCSI.

logiciel iSCSI Votre hôte utilise un initiateur iSCSI logiciel dans le VMkernel pour se connecter au stockage. Avec ce type de connexion iSCSI, votre hôte ne requiert qu'un adaptateur réseau standard pour la connectivité réseau.

Stockage relié au réseau (NAS) Stocke les fichiers de machine virtuelle sur des serveurs de fichiers à distance accessibles sur un réseau TCP/IP standard. Le client NFS intégré dans ESX utilise le protocole NFS (Network File System) version 3 pour communiquer avec les serveurs NAS/NFS. Pour une connectivité réseau, l'hôte requiert un adaptateur réseau standard.

SAS (Serial Attached SCSI) partagé Stocke des machines virtuelles sur des systèmes de stockage directement reliés au SAS qui offrent un accès partagé à plusieurs hôtes. Ce type d'accès permet à plusieurs hôtes d'accéder à la même banque de données VFMS sur un LUN.

Adaptateurs de stockage pris en charge

Les adaptateurs de stockage fournissent une connectivité pour votre hôte ESX à un réseau ou une unité de stockage spécifique.

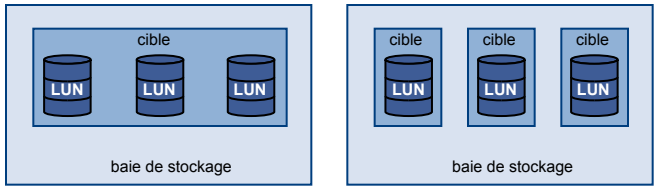
Selon le type de stockage utilisé, vous devez peut-être installer ou activer un adaptateur de stockage sur votre hôte. ESX prend en charge différentes catégories d'adaptateurs, y compris SCSI, iSCSI, RAID, Fibre Channel, Fibre Channel over Ethernet (FCoE) et Ethernet. ESX accède directement aux adaptateurs via des pilotes de périphériques dans le VMkernel.

Représentations de périphériques et de cibles

Dans un environnement ESX, le terme cible identifie une unité de stockage unique à laquelle accède l'hôte. Les termes périphérique et LUN décrivent un volume logique qui représente l'espace de stockage sur une cible. En général, les termes périphérique et LUN, dans un contexte ESX, signifient qu'un volume SCSI est présenté à l'hôte depuis une unité de stockage cible et disponible pour un formatage.

Différents fournisseurs de stockage présententntntnt les systèmes de stockage pour les hôtes ESX de différentes manières. Certains fournisseurs présentent une cible unique comportant plusieurs LUN ou périphériques de stockage, tandis que d'autres proposent plusieurs cibles disposant chacune d'un LUN.

Figure 7-1. Représentations LUN et de cibles



Dans cette illustration, trois LUN sont disponibles pour chaque configuration. Dans un cas, l'hôte voit une cible, mais cette cible comporte trois LUN à utiliser. Chaque LUN représente un volume de stockage individuel. Dans l'autre exemple, l'hôte voit trois cibles différentes, chacune disposant d'un LUN.

Les cibles accessibles via le réseau ont des noms uniques fournis par les systèmes de stockage. Les cibles iSCSI utilisent des noms iSCSI, tandis que les cibles Fibre Channel utilisent des noms mondiaux dits Noms mondials (WWN).

Remarque ESX ne prend en charge pas l'accès au même LUN via différents protocoles de transport, tels que iSCSI et Fibre Channel.

Un périphérique, ou LUN, est identifié par son nom UUID. Si un LUN est partagé par plusieurs hôtes, il doit être présenté à tous les hôtes ayant le même UUID.

Explication du nommage Fibre Channel

Dans un SAN Fibre Channel, un nom ditNom mondial WWN identifie de manière unique chaque élément dans le réseau, tel que le périphérique de stockage ou l'adaptateur Fibre Channel.

Le nom WWN est une adresse à 64 octets comportant 16 nombres hexadécimaux et prend la forme suivante :

```
20:00:00:e0:8b:8b:38:77 21:00:00:e0:8b:8b:38:77
```

Le nom WWN est affecté à chaque élément Fibre Channel SAN par son fabricant.

Comprendre la dénomination et l'adressage iSCSI

Dans un réseau iSCSI, chaque élément iSCSI qui utilise le réseau possède un nom iSCSI unique et permanent, et une adresse d'accès lui est attribuée.

nom iSCSI

Identifie un élément iSCSI particulier, indépendamment de son emplacement physique. Le nom iSCSI peut utiliser le format IQN ou EUI.

- IQN (iSCSI Qualified Name). Peut compter jusqu'à 255 caractères, au format suivant :

  `iqn.aaaa-mm.autorité-dénomination:nom unique`

aaaa-mm	L'année et le mois où l'autorité de dénomination a été établie.
autorité-dénomination	Syntaxe habituellement inverse du nom de domaine Internet de l'autorité de dénomination. Par exemple, l'autorité de dénomination iscsi.vmware.com pourrait porter le nom qualifié iSCSI sous la forme iqn. 1998-01.com.vmware.iscsi. Ce nom indique que le nom de domaine vmware.com a été inscrit en janvier 1998, et que iscsi est un sous-domaine, dirigé par vmware.com.
nom unique	N'importe quel nom à votre guise, par exemple le nom de votre hôte. L'autorité de dénomination doit s'assurer que tous les éventuels noms attribués après les deux-points sont uniques. Par exemple, `iqn. 1998-01.com.vmware.iscsi:nom1`.

- EUI (Extended Unique Identifier). Inclut le préfixe `eui.`, suivi du nom de 16 caractères. Le nom comporte 24 bits pour le nom de la société attribué par l'IEEE, et 40 bits pour un identifiant unique, tel qu'un numéro de série.

  Par exemple,

  `eui.0123456789ABCDEF`

Alias iSCSI

Nom plus parlant et plus facile à retenir que le nom iSCSI. Les alias iSCSI, qui ne sont pas uniques, sont destinés à n'être qu'un surnom à associer au noeud.

Adresse IP

Adresse associée à chaque élément iSCSI de sorte que le matériel d'acheminement et de commutation du réseau puisse établir la connexion entre différents éléments, tels que l'hôte et le stockage. Ceci est en fait similaire à l'adresse IP que vous attribuez à un ordinateur pour bénéficier de l'accès au réseau de votre entreprise ou à Internet.

Explication du nommage de périphériques de stockage

Dans le vSphere Client, chaque périphérique de stockage ou LUN est identifié par plusieurs noms, y compris un surnom, un nom UUID et un nom d'exécution.

Nom

C'est un surnom que l'hôte ESX affecte à un périphérique selon le type de stockage et le fabricant. Vous pouvez modifier le nom à l'aide de vSphere Client. Lorsque vous modifiez le nom du périphérique sur un hôte, le changement prend effet sur tous les hôtes ayant accès à ce périphérique.

Identificateur

C'est un identificateur universel unique attribué à un périphérique. Selon le type de stockage, différents algorithmes sont utilisés pour créer l'identificateur. L'identificateur est permanent à travers les redémarrages et doit être identique pour tous les hôtes partageant le périphérique.

Nom d'exécution

C'est le nom du premier chemin d'accès au périphérique. Le nom d'exécution est créé par l'hôte, ce n'est pas un identificateur fiable pour le périphérique et il n'est pas permanent.

Le nom d'exécution a le format suivant : `vmhba#:C#:T#:L#`.

vmhba# Nom de l'adaptateur de stockage. Le nom fait référence à la carte physique sur l'hôte et non au contrôleur SCSI utilisé par les machines virtuelles.

C# Numéro du canal de stockage. Les initiateurs iSCSI logiciels utilisent le numéro de canal pour présenter plusieurs chemins menant à la même cible.

T# Numéro de la cible. La numérotation de la cible est choisie par l'hôte et peut être modifiée en cas de changement de mappages des cibles visibles par l'hôte. Il se peut que des cibles partagées par différents hôtes ESX n'aient pas le même numéro de cible.

L# Numéro de LUN montrant la position du LUN dans la cible. Le numéro de LUN est fourni par le système de stockage. Si une cible possède un seul LUN, le numéro de LUN est toujours zéro (0).

Par exemple, `vmhba1:C0:T3:L1` représente LUN1 sur la cible 3 accessible via l'adaptateur de stockage vmhba1 et le canal 0.

À propos des banque de données ESX

Les banque de données sont des conteneurs logiques, analogues à des systèmes de fichiers, qui masquent les informations de chaque périphérique de stockage et fournissent un modèle uniforme pour stocker des fichiers de machine virtuelle. Les banque de données peuvent également être utilisées pour le stockage d'images ISO, de modèles de machine virtuelle et d'images de disquette.

Vous utilisez le vSphere Client Client pour accéder aux différents types de périphériques de stockage que votre hôteESX découvre, et y déployer des banque de données.

Selon le type de stockage utilisé, les banque de données peuvent être sauvegardées aux formats de système de fichier suivants :

Système de fichier de la machine virtuelle (VMFS) Système de fichier haute performance optimisé pour le stockage de machines virtuelles. Votre hôte peut déployer une banque de données VMFS sur un périphérique de stockage en réseau ou local SCSI, y compris des équipements Fibre Channel et iSCSI SAN.

Au lieu d'utiliser la banque de données VMFS, votre machine virtuelle peut directement accéder aux périphériques bruts et utiliser un fichier de mappage (RDM) comme proxy.

Système de fichier du réseau (NFS) Système de fichier sur un périphérique de stockage NAS. ESX prend en charge uniquement NFS version 3 sur TCP/IP. L'hôte peut accéder à un volume NFS dédié, situé sur un serveur NFS, monter le volume et l'utiliser pour des besoins de stockage.

Si vous utilisez la console de service pour accéder à votre hôte ESX, vous pouvez voir les banque de données NFS et VMFS en tant que sous-répertoires distincts dans l'inventaire `/vmfs/volumes`.

Banques de données VMFS

ESX peut formater des périphériques de stockage SCSI tels que des banques de données VMFS. Les banques de données VMFS servent principalement de référentiel aux machines virtuelles.

Vous pouvez stocker plusieurs machines virtuelles sur le même volume VMFS. Chaque machine virtuelle, encapsulée dans un ensemble de fichier, occupe un répertoire unique et distinct. Pour le système d'exploitation au sein de la machine virtuelle, VMFS conserve la sémantique du système de fichiers interne, qui garantit un comportement d'application adéquat et une intégrité des données pour les applications s'exécutant dans les machines virtuelles.

Par ailleurs, vous pouvez utiliser les banque de données VMFS pour stocker d'autres fichiers, tels que des modèles de machine virtuelle et des images ISO.

VMFS prend en charge les tailles de verrouillage et de fichiers suivantes, permettant ainsi aux machines virtuelles de pouvoir aussi exécuter des applications utilisant beaucoup de données, y compris des bases de données, des progiciels de gestion intégrés (ERP) et des gestions de relations (CRM) dans des machines virtuelles :

- Taille max. disque virtuel : 2 To, taille verr. 8 Mo
- Taille max fichier : 2 To, taille verr. 8 Mo
- Taille. verr. : 1 Mo (par défaut), 2 Mo, 4 Mo et 8 Mo

Création et agrandissement des banques de données VMFS

Vous pouvez configurer des banque de données VMFS sur des périphériques de stockage SCSI que votre hôte ESX découvre. Après avoir créé la banque de données VMFS, vous pouvez modifier ses propriétés.

Vous pouvez posséder jusqu'à 256 banque de données par système, avec une taille de volume minimale de 1,2 Go.

REMARQUE Ayez toujours une seule banque de données VMFS par LUN.

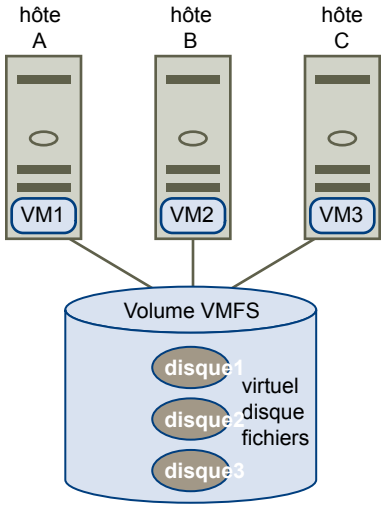
Si votre banque de données VMFS requiert plus d'espace, vous pouvez augmenter le volume VMFS. Vous pouvez dynamiquement ajouter de nouvelles extensions à une banque de données VMFS et agrandir la banque de données jusqu'à 64 To. Une extension est un LUN ou partition sur un périphérique de stockage physique. La banque de données peut s'étirer sur plusieurs extensions, et apparaître en tant que volume unique.

Une autre option consiste à agrandir l'extension de la banque de données existante si le périphérique de stockage où réside votre banque de données a de l'espace libre. Vous pouvez agrandir l'extension jusqu'à 2 To.

Partager un volume VMFS par le biais d'hôtes ESX

En tant que système de fichiers cluster, VMFS permet à plusieurs hôtes ESX d'accéder à la même banque de données VMFS simultanément. Vous pouvez connecter jusqu'à 32 hôtes à un volume VMFS unique.

Figure 7-2. Partager un volume VMFS par le biais d'hôtes



Pour garantir que la même machine virtuelle ne soit pas accédée par plusieurs serveurs simultanément, VMFS fournit un verrouillage sur disque.

Le partage du même volume VMFS par le biais de plusieurs hôtes offre les avantages suivants :

- Vous pouvez utiliser VMware Distributed Resource Scheduling et VMware High Availability.

  Vous pouvez distribuer des machines virtuelles à travers différents serveurs physiques. Cela signifie que vous exécutez un mélange de machines virtuelles sur chaque serveur de sorte qu'il ne reçoive pas de demandes trop importantes dans la même zone, simultanément. Si un serveur échoue, vous pouvez redémarrer les machines virtuelles sur un autre serveur physique. En cas de défaillance, le verrouillage sur disque pour chaque machine virtuelle s'active.

- Vous pouvez utiliser vMotion pour migrer des machines virtuelles en cours d'exécution depuis un serveur physique vers un autre.

- Vous pouvez utiliser VMware Consolidated Backup qui permet à un serveur proxy, appelé proxy VCB, de sauvegarder la capture instantanée d'une machine virtuelle tandis que cette dernière est sous tension ou lit/écrit sur son stockage.

Banque de données NFS

L'hôte ESX peut accéder à un volume NFS dédié, situé sur un serveur NAS, monter le volume et l'utiliser pour des besoins de stockage. Vous pouvez utiliser des volumes NFS pour stocker et démarrer des machines virtuelles de la même manière que vous utilisez des banques de données VMFS.

ESX prend en charge les capacités de stockage partagé suivantes sur des volumes NFS :

- vMotion
- VMware DRS et VMware HA
- Images ISO, présentées en tant que CD-ROM aux machines virtuelles
- Snapshots instantanées de machine virtuelle

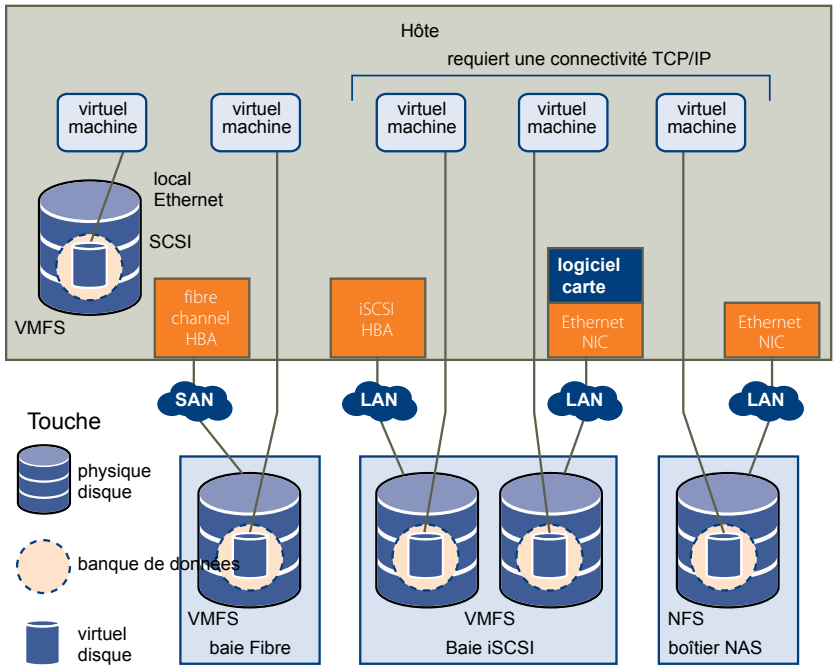
Accès des machines virtuelles au stockage

Lorsqu'une machine virtuelle communique avec son disque virtuel stocké sur une banque de données, elle lance des commandes SCSI. Étant donné que les banque de données peuvent résider sur plusieurs types de stockage physique, ces commandes sont encapsulées dans d'autres formes, selon le protocole utilisé par l'hôte ESX pour se connecter à un périphérique de stockage.

ESX prend en charge les protocoles Fibre Channel (FC), SCSI Internet (iSCSI), Fibre Channel over Ethernet (FCoE) et NFS. Quel que soit le type de périphérique de stockage utilisé par votre hôte, le disque virtuel apparaît toujours en tant que périphérique SCSI monté pour la machine virtuelle. Le disque virtuel masque une couche de stockage physique au système d'exploitation de la machine virtuelle. Cette action permet d'exécuter des systèmes d'exploitation non certifiés pour un équipement de stockage spécifique, tel que SAN, dans une machine virtuelle.

Figure 7-3 décrit cinq machines virtuelles utilisant différents types de stockage afin d'illustrer leurs différences.

Figure 7-3. Machines virtuelles accédant à différents types de stockage



Remarque Ce diagramme est uniquement destiné à des fins conceptuelles. Ce n'est pas une configuration recommandée.

Comparaison des types de stockage

La prise en charge de certaines fonctionnalités de vSphere peut dépendre de la technologie de stockage que vous utilisez.

Tableau 7-1 compare les technologies de stockage en réseau pris en charge par ESX.

Tableau 7-1. Stockage en réseau pris en charge par ESX

Technologie	Protocoles	Transferts	Interface
Fibre Channel	FC/SCSI	Bloquer l'accès de données/ LUN	FC HBA
iSCSI	IP/SCSI	Bloquer l'accès de données/ LUN	■ iSCSI HBA (iSCSI matérielle) ■ NIC (iSCSI logiciel)
NAS	IP/NFS	Fichier (pas d'accès direct à LUN)	NIC

Tableau 7-2 compare les fonctionnalités de vSphere pris en charge par différents types de stockage.

Tableau 7-2. Fonctions vSphere pris en charge par le stockage

Type de stockage	Démarrage VM	vMotion	Banque de données	RDM	Cluster VM	VMware HA et DRS	VCB
Stockage local	Oui	Non	VMFS	Non	Non	Non	Oui
Fibre Channel	Oui	Oui	VMFS	Oui	Oui	Oui	Oui
iSCSI	Oui	Oui	VMFS	Oui	Oui	Oui	Oui
NAS sur NFS	Oui	Oui	NFS	Non	Non	Oui	Oui

Afficher les adaptateurs de stockage

L'hôte utilise des adaptateurs de stockage pour accéder aux différents périphériques de stockage. Vous pouvez afficher les adaptateurs de stockage disponibles et consulter leurs informations.

Tableau 7-3 recense les informations que vous pouvez consulter quand vous affichez les détails sur chaque adaptateur. Certains adaptateurs, par exemple iSCSI, doivent être configurés ou activés avant de pouvoir en consulter les informations.

Tableau 7-3. Informations sur les adaptateurs de stockage

Informations sur les adaptateurs	Description
Modèle	Modèle de l'adaptateur.
Cibles (Fibre Channel et SCSI)	Nombre de cibles auxquelles il a été accédé via l'adaptateur.
Cibles connectées (iSCSI)	Nombre de cibles connectées sur un adaptateur iSCSI.
WWN (Fibre Channel)	Nom mondial formé selon les normes Fibre Channel qui identifie de manière univoque l'adaptateur FC.
Nom iSCSI (iSCSI)	Nom unique formé selon les normes iSCSI qui identifie l'adaptateur iSCSI.
Alias iSCSI (iSCSI)	Surnom utilisé au lieu du nom iSCSI.
Adresse IP (iSCSI matérielle)	Adresse assignée à l'adaptateur iSCSI.
Méthodes de découverte (iSCSI)	Méthodes de découverte que l'adaptateur iSCSI applique pour accéder aux cibles iSCSI.
Périphériques	Tous les périphériques de stockage ou LUN auxquels l'adaptateur peut accéder.
Chemins d'accès	Tous les chemins que l'adaptateur l'utilise pour accéder aux périphériques de stockage.

Consulter les informations sur les adaptateurs de stockage

Vous pouvez afficher les adaptateurs de stockage dont se sert votre hôte et consulter leurs informations.

Procédure

1 Dans l'inventaire, sélectionnez **[Hôtes et clusters]** .

2 Sélectionnez un hôte et cliquez sur l'onglet **[Configuration]** .

3 Dans Matériel, sélectionnez **[Adaptateurs de stockage]** .

4 Pour afficher les détails sur un adaptateur particulier, sélectionnez-le dans la liste d'adaptateurs de stockage.

5 Pour répertorier tous les périphériques de stockage auxquels l'adaptateur peut accéder, cliquez sur **[Périphériques]** .

6 Pour répertorier tous les chemins qu'utilise l'adaptateur, cliquez sur **[Chemins]** .

Copier des identifiants d'adaptateur de stockage dans le presse-papiers

Si vos adaptateurs de stockage utilisent des identifiants uniques, tels qu'un nom iSCSI ou un WWN, vous pouvez les copier dans un presse-papiers directement à partir de l'interface.

Procédure

1 Dans l'inventaire, sélectionnez **[Hôtes et clusters]** .

2 Sélectionnez un hôte et cliquez sur l'onglet **[Configuration]** .

3 Dans Matériel, sélectionnez **[Adaptateurs de stockage]** .

4 Sélectionnez l'adaptateur dans la liste d'adaptateurs de stockage.

5 Dans le panneau Détails, cliquez avec le bouton droit sur la valeur dans le champ de nom, et sélectionnez **[Copier]** .

Afficher les périphériques de stockage

Vous pouvez afficher tous les périphériques de stockages ou LUN disponibles pour l'hôte, y compris tous les périphériques en réseau et locaux. Si vous utilisez des plug-ins multichemins tiers, les périphériques de stockage disponibles via les plug-ins apparaissent également dans la liste.

Pour chaque adaptateur de stockage, vous pouvez afficher une liste distincte de périphériques de stockage disponibles pour cet adaptateur.

En règle générale, lorsque vous consultez les périphériques de stockages, vous voyez les informations suivantes.

Tableau 7-4. Informations du périphérique de stockage

Informations du périphérique de stockage	Description
Nom	Surnom que l'hôte ESX affecte à un périphérique selon le type de stockage et le fabricant. Vous pouvez changer ce nom par le nom de votre choix.
Identificateur	Identificateur universel unique intrinsèque au périphérique.
Nom d'exécution	Nom du premier chemin d'accès au périphérique.
LUN	Numéro de LUN montrant la position du LUN dans la cible.
Type	Type de périphérique, par exemple, disque ou CD-ROM.

Tableau 7-4. Informations du périphérique de stockage (suite)

Informations du périphérique de stockage	Description
Transport	Protocole de transport utilisé par votre hôte pour accéder au périphérique.
Capacité	Capacité totale du périphérique de stockage.
Propriétaire	Plugin, comme le NMP ou un plugin tiers, utilisé par l'hôte pour gérer le périphérique de stockage.
Accélération matérielle	Informations indiquant que le périphérique de stockage assiste l'hôte avec des opérations de gestion de machine virtuelle. L'état peut être Pris en charge, Non pris en charge ou Inconnu. Pour des détails, veuillez vous reporter à la section « Accélération matérielle du stockage », page 136.
Emplacement	Chemin d'accès au périphérique de stockage dans l'inventaire `/vmfs/devices/`.
Partitions	Partitions logiques et principales, y compris une banque de données VMFS, si configurée.

Affichage des périphériques de stockage d'un hôte

Vous pouvez afficher tous les périphériques de stockage ou LUN disponibles pour un hôte. Si vous utilisez des plug-ins multichemins tiers, les périphériques de stockage disponibles via les plug-ins apparaissent également dans la liste.

Procédure

1 Dans l'inventaire, sélectionnez **[Hôtes et clusters]** .

2 Sélectionnez un hôte et cliquez sur l'onglet **[Configuration]** .

3 Dans Matériel, sélectionnez **[Stockage]** .

4 Cliquez sur **[Périphériques]** .

5 Pour afficher des informations complémentaires sur un périphérique spécifique, sélectionnez le périphérique à partir de la liste.

Affichage des périphériques de stockage d'un adaptateur

Vous pouvez afficher une liste des périphériques de stockage accessibles à un adaptateur de stockage spécifique sur l'hôte.

Procédure

1 Dans l'inventaire, sélectionnez **[Hôtes et clusters]** .

2 Sélectionnez un hôte et cliquez sur l'onglet **[Configuration]** .

3 Dans Matériel, sélectionnez **[Adaptateurs de stockage]** .

4 Sélectionnez l'adaptateur dans la liste d'adaptateurs de stockage.

5 Cliquez sur **[Périphériques]** .

Copier des identificateurs de périphérique de stockage dans le presse-papiers

Un identificateur de périphérique de stockage est un ID universelle unique attribuée à un périphérique de stockage ou LUN. Selon le type de stockage, différents algorithmes sont utilisés pour créer l'identificateur et il peut être long et complexe. Vous pouvez directement copier l'identificateur de périphérique de stockage depuis l'interface utilisateur.

Procédure

1 Affichez la liste des périphériques de stockage.

2 Cliquez avec le bouton droit de la souris sur un périphérique, puis sélectionnez **[Copier identifiant dans le presse-papier]** .

Affichage de banques de données

Vous pouvez afficher toutes les banque de données disponibles pour vos hôtes et analyser leurs propriétés.

Les banques de données sont ajoutées à vSphere Client de la façon suivante :

- banque de données créées sur un périphérique de stockage disponible.
- Reconnaissance en cas d'ajout d'hôte à l'inventaire. Lorsque vous ajoutez un hôte à l'inventaire, vSphere Client affiche les banque de données disponibles pour l'hôte.

Si votre vSphere Client est connecté à un système vCenter Server, vous pouvez afficher des informations sur les banques de données dans la vue banque de données. Cette vue affiche tous les banques de données de l'inventaire, organisées par centre de données. Grâce à cette vue, vous pouvez organiser des banques de données dans une hiérarchie de fichiers, créer des banques de données, modifier leurs propriétés ou supprimer des banques de données existantes.

Cette vue est complète et affiche toutes les informations de vos banque de données, y compris les hôtes et machines virtuelles les utilisant, les informations de rapports de stockage, les autorisations, les alarmes, les tâches et événements, la topologie de stockage, et les rapports de stockage. Des informations de configuration pour chaque banque de données sur tous les hôtes qui y sont connectés sont fournies dans l'onglet Configuration de la vue banque de données.

Remarque La vue banque de données n'est pas disponible quand le vSphere Client se connecte directement à votre hôte. Dans ce cas, consultez les informations de banque de données via l'onglet de configuration de stockage de l'hôte.

Tableau 7-5 fournit des informations détaillées sur la banque de données que vous pouvez consulter lorsque vous effectuez une analyse de banques de données.

Tableau 7-5. Informations sur les banque de données

Informations sur les banque de données	Description
Identification	Nom modifiable affecté à la banque de données.
Périphérique	Périphérique de stockage sur lequel est déployée la banque de données.
Capacité	Capacité totale formatée de la banque de données.
Espace	libre disponible.
Type	Système de fichiers utilisé par la banque de données (VMFS ou NFS).
Contrôle d'E/S de stockage	Permet la gestion des priorités d'E/S de stockage. Voir le *guide de gestion des ressources vSphere*.

Tableau 7-5. Informations sur les banque de données (suite)

Informations sur les banque de données	Description
Accélération matérielle	Informations indiquant que la banque de données assiste l'hôte avec des opérations de gestion de machine virtuelle. L'état peut être Pris en charge, Non pris en charge ou Inconnu. Pour des détails, veuillez vous reporter à la section « Accélération matérielle du stockage », page 136.
Emplacement	Chemin d'accès à la banque de données dans l'inventaire `/vmfs/volumes/`.
Extensions	Extensions de la banque de données et capacité correspondante (banque de données VMFS uniquement).
Sélection de chemin d'accès	Règles de sélection de chemin d'accès utilisées par l'hôte pour accéder aux espaces de stockage (banque de données VMFS uniquement).
Chemins d'accès	Nombre de chemins d'accès utilisés pour accéder au stockage et leur statut (banque de données VMFS uniquement).

Consulter les propriétés des banque de données

Vous pouvez afficher toutes les banque de données disponibles pour les hôtes et analyser leurs propriétés.

Procédure

1 Affichez l'hôte dans l'inventaire.

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

3 Dans Matériel, sélectionnez **[Stockage]** .

4 Cliquez sur la vue **[banque de données]** .

5 Pour afficher les informations sur une banque de données spécifique, sélectionnez la banque de données à partir de la liste.

Configurer le stockage ESX 8

La rubrique suivante contient les informations de configuration des périphériques de stockage SCSI locaux, du stockage Fibre Channel SAN, du stockage iSCSI et du stockage NFS.

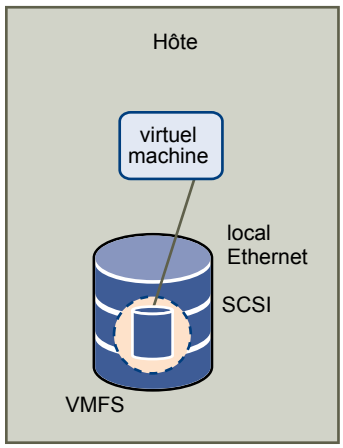
Ce chapitre aborde les rubriques suivantes :

Stockage SCSI local

Le stockage local emploie un périphérique SCSI tel que le disque dur de votre hôte ESX ou tout autre système de stockage externe connecté directement à votre hôte.

Figure 8-1 décrit une machine virtuelle utilisant un stockage SCSI local.

Figure 8-1. Stockage local



Dans cet exemple de topologie de stockage local, l'hôte ESX emploie une connexion unique à un disque. Sur ce disque, vous pouvez créer une banque de données VMFS que vous utilisez pour stocker les fichiers de disque de la machine virtuelle.

Bien que cette configuration de stockage soit possible, cette topologie n'est pas recommandée. L'utilisation de connexions uniques entre des baies de stockage et des hôtes crée des points de défaillance uniques (SPOF) pouvant causer des interruptions lorsqu'une connexion devient instable ou échoue.

Afin de garantir une tolérance aux pannes, certains systèmes DAS prend en chargent des chemins de connexion redondants.

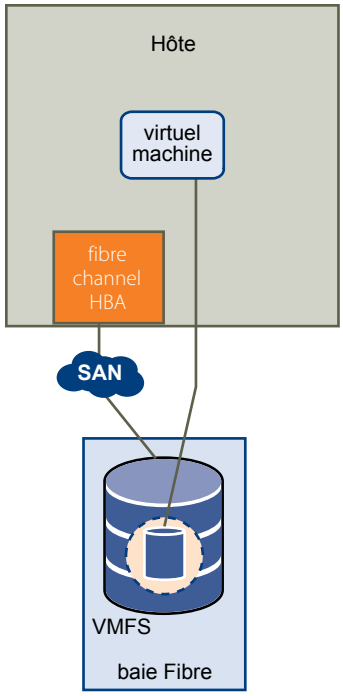
Stockage Fibre Channel

ESX prend en charge les cartes Fibre Channel permettant à un hôte de se connecter au SAN et d'afficher les périphériques de stockage sur le SAN.

Vous devez installer des cartes Fibre Channel (FC) pour que l'hôte puisse accéder aux périphériques de stockage FC.

Figure 8-2 décrit les machines virtuelles utilisant le stockage Fibre Channel.

Figure 8-2. Stockage Fibre Channel



Dans cette configuration, un hôte ESX se connecte à une structure SAN composée de baies de stockage et de commutateurs Fibre Channel, via un adapteur Fibre Channel. Les LUN d'une baie de stockage deviennent disponibles pour l'hôte. Vous pouvez accéder aux LUN et créer une banque de données pour vos besoins de stockage. La banque de données utilise le format VMFS.

Pour des informations spécifiques sur la configuration de la structure SAN FC et des baies de stockage pour ESX, consultez le *guide de configuration Fibre Channel SAN*.

Stockage iSCSI

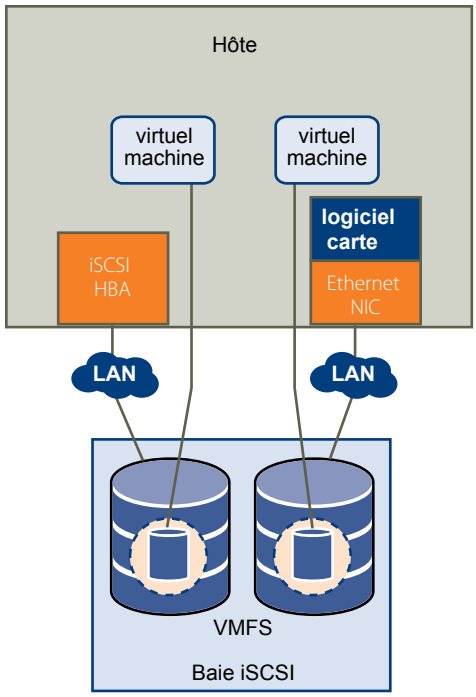
ESX prend en charge la technologie iSCSI qui permet à votre hôte d'employer un réseau IP pour accéder au stockage à distance. Avec iSCSI, le stockage SCSI impose que les communications de votre machine virtuelle vers son disque virtuel soient converties en paquets TCP/IP et transmises à un périphérique distant, ou cible, qui stocke le disque virtuel.

Pour accéder aux cibles distantes, votre hôte emploie des initiateurs iSCSI. Les initiateurs transportent les requêtes et réponses SCSI entre l'hôte et le périphérique de stockage cible sur le réseau IP. ESX prend en charge les initiateurs iSCSI matériels, dépendants et indépendants, et logiciels.

Vous devez configurer les initiateurs iSCSI de l'hôte pour qu'il accède et affiche les périphériques de stockage iSCSI.

Figure 8-3 décrit les différents types d'initiateurs iSCSI.

Figure 8-3. Stockage iSCSI



Dans l'exemple de gauche, l'hôte utilise la carte iSCSI matérielle pour se connecter au système de stockage iSCSI.

Dans l'exemple de droite, l'hôte utilise un adapteur iSCSI logiciel et un adapteur d'interface réseau Ethernet pour se connecter au stockage iSCSI.

Les périphériques de stockage iSCSI du système de stockage deviennent disponibles pour l'hôte. Vous pouvez accéder aux périphériques de stockage et créer des banque de données VMFS pour vos besoins de stockage.

Pour des informations spécifiques sur la configuration de la structure SAN iSCSI pour fonctionner avec ESX, consultez le *guide de configuration iSCSI SAN*.

Initiateurs iSCSI

Pour accéder aux cibles iSCSI, votre hôte utilise des initiateurs iSCSI. Les initiateurs transportent les requêtes et réponses SCSI, encapsulées dans le protocole iSCSI, entre l'hôte et la cible iSCSI.

VMware prend en charge plusieurs types d'initiateurs.

Adaptateur de logiciel iSCSI

Un adaptateur de logiciel ISCSI est un code vMware intégré au VMKernel. Il permet à un hôte de se connecter au périphérique de stockage iSCSI par des cartes réseau standard. L'adaptateur de logiciel ISCSI gère le traitement iSCSI tout en communiquant avec l'adaptateur réseau. Avec l'adaptateur de logiciel ISCSI, vous pouvez employer la technologie iSCSI sans acheter de matériel spécialisé.

Adaptateur de matériel ISCSI

Un adaptateur de matériel ISCSI est un adaptateur tiers qui déchargre le traîtement ISCSI et le réseau de votre hôte. Les adaptateurs matériels iSCSI se divisent en plusieurs catégories.

Adaptateur de matériel ISCSI dépendant

Dépend du réseau VMware et des interfaces de configuration et de gestion iSCSI fournies par VMware.

Ce type d'adaptateur peut être un adaptateur réseau standard disposant de la fonction de déchargement iSCSI pour le même port. La fonction de déchargement iSCSI dépend de la configuration du réseau pour obtenir les paramètres IP, MAC et d'autres paramètres utilisés pour les sessions iSCSI. La carte NIC Broadcom 5709 sous licence iSCSI est un exemple d'adaptateur dépendant.

Adaptateur de matériel ISCSI indépendant

Implémente ses propres protocoles réseau et ses propres interfaces de configuration et de gestion iSCSI.

Une carte disposant uniquement de la fonction de déchargement iSCSI ou de la fonction de déchargement iSCSI et NIC standard est un exemple d'adaptateur iSCSI matériel indépendant. La fonction de déchargement iSCSI dispose d'une fonction de gestion indépendante de la configuration, qui assigne les paramètres IP, MAC et d'autres paramètres pour les sessions iSCSI. L'adaptateur QLogic QLA4052 est un exemple d'adaptateur indépendant.

Les adaptateurs de matériel ISCSI doivent avoir une licence. Sinon, ils n'apparaîtront pas dans vSphere Client ou vSphere CLI. Contactez votre fournisseur pour avoir des renseignements sur la licence.

Configurer des adaptateurs iSCSI matériels indépendants

Un adaptateur iSCSI matériel indépendant est un adaptateur tiers spécialisé capable d'accéder au stockage iSCSI via TCP/IP. Cet adaptateur iSCSI s'occupe de tout le traitement et de toute la gestion iSCSI et réseau de votre système ESX.

La procédure complète d'installation et de configuration des adaptateurs iSCSI matériels indépendants comprend les étapes suivantes :

1 Vérifiez si l'adaptateur doit faire l'objet d'une licence.

   Consultez la documentation du fabricant.

2 Installez l'adaptateur.

   Pour toute information sur l'installation, consultez la documentation du fabricant.

3 Assurez-vous que l'adaptateur est correctement installé.

   Reportez-vous à « Afficher des adaptateurs iSCSI matériels indépendants », page 103.

4 Configurez les adresses de découverte.

   Reportez-vous à « Configurer des adresses de découverte pour des initiateurs iSCSI », page 108.

5 Configurez les paramètres CHAP.

   Reportez-vous à « Configurer des paramètres CHAP pour des cartes iSCSI », page 109.

Pour que votre hôte puisse accéder au stockage iSCSI, vous devez d'abord installer l'adaptateur iSCSI matériel et configurer l'adresse de découverte et les paramètres CHAP.

Afficher des adaptateurs iSCSI matériels indépendants

Affichez un adaptateur iSCSI matériel pour vérifier qu'il est correctement installé et prêt pour la configuration.

Prérequis

Une fois que vous avez installé un adaptateur iSCSI matériel, il apparaît dans la liste des adaptateurs de stockage disponibles pour la configuration. Vous pouvez consulter ses propriétés.

Privilège nécessaire :**Hôte.Configuration.Configuration de partition de stockage**

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez un hôte dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Adaptateurs de stockage]** dans le panneau Matériel.

S'il est installé, l'initiateur iSCSI matériel doit figurer dans la liste d'adaptateurs de stockage.

3 Sélectionnez l'initiateur à consulter.

Les détails par défaut de l'initiateur apparaissent, y compris le modèle, le nom iSCSI, l'alias iSCSI, l'adresse IP ainsi que les informations sur la cible et les chemins.

4 Cliquez sur **[Propriétés]** .

La boîte de dialogue de propriétés d'initiateur iSCSI apparaît. L'onglet **[Général]** affiche des caractéristiques complémentaires sur l'initiateur.

Vous pouvez maintenant configurer votre initiateur matériel ou modifier ses caractéristiques par défaut.

Modifier le nom et l'adresse IP des initiateurs matériels indépendants

Quand vous configurez vos initiateurs de matériel iSCSI indépendants, assurez-vous que leurs noms et adresses IP sont formatés correctement.

Procédure

1 Accédez à la boîte de dialogue de propriétés d'initiateur iSCSI.

2 Cliquez sur **[Configurer]** .

3 Pour changer le nom iSCSI par défaut pour votre initiateur, entrez le nouveau nom.

Assurez-vous que le nom que vous entrez est unique mondialement et correctement formaté ou certains périphériques de stockage pourraient ne pas identifier l'initiateur du matériel iSCSI.

4 (Facultatif) Entrez l'alias iSCSI.

L'alias est un nom que vous utilisez pour identifier l'initiateur du matériel iSCSI.

5 Changez les paramètres IP par défaut.

Vous devez modifier les paramètres IP par défaut pour qu'ils soient configurés correctement pour le réseau de stockage IP. Travaillez avec votre administrateur réseau pour déterminer le paramètre IP pour le HBA.

6 Cliquez sur **[OK]** pour enregistrer vos modifications.

Si vous changez le nom iSCSI, celui-ci sera utilisé pour de nouvelles sessions iSCSI. Pour des sessions existantes, les nouveaux paramètres ne seront pas utilisés jusqu'à la déconnexion et la reconnexion.

Installation et configuration d'un adaptateur iSCSI logiciel

Avec l'implémentation iSCSI logiciel, vous pouvez utiliser des cartes réseau standards pour connecter votre hôte à une cible iSCSI distante sur le réseau IP. L'adaptateur iSCSI logiciel compris dans ESX facilite cette connexion en communicant avec les NIC physiques par la pile réseau.

Quand vous vous connectez à vCenter Server ou à un hôte avec vSphere Client, l'adaptateur iSCSI logiciel apparaît dans la liste de vos adaptateurs de stockage. Un seul adaptateur iSCSI logiciel apparaît. Pour pouvoir utiliser l'adaptateur iSCSI logiciel, vous devez d'abord installer le réseau, activer l'adaptateur, et configurer les paramètres tels que les adresses de découvertes et le CHAP. Le workflow de configuration de l'adaptateur iSCSI logiciel comprend les étapes suivantes :

1 Configurez le réseau iSCSI en créant des ports pour le trafic iSCSI.

  Reportez-vous à « Configuration du réseau pour l'iSCSI logiciel et l'iSCSI matériel dépendant », page 75.

2 Activez l'adaptateur iSCSI.

  Reportez-vous à « Activer l'adaptateur iSCSI logiciel », page 104.

3 Si vous utilisez des NIC multiples pour le multichemin iSCSI logiciel, associez les ports en connectant tous les ports iSCSI à l'adaptateur iSCSI logiciel.

  Reportez-vous à « Associer des ports iSCSI aux adaptateurs iSCSI », page 107.

4 Si nécessare, activez les trames Jumbo. Les Trames jumbo doivent être activées pour chaque vSwitch par le vSphere CLI. Vous devez également, si vous utilisez un hôte ESX, créer une interface réseau VMkernel avec ses Trames jumbo activées.

  Reportez vous à la section *Mise en réseau* pour plus d'informations.

5 Configurez les adresses de découverte.

  Reportez-vous à « Configurer des adresses de découverte pour des initiateurs iSCSI », page 108.

6 Configurez les paramètres CHAP.

  Reportez-vous à « Configurer des paramètres CHAP pour des cartes iSCSI », page 109.

Activer l'adaptateur iSCSI logiciel

Vous devez activer votre adaptateur iSCSI logiciel avant que votre hôte puisse l'utiliser pour accéder au stockage iSCSI.

Prérequis

Avant d'activer l'adaptateur iSCSI logiciel, installez le réseau pour l'iSCSI.

Remarque Si vous démarrez depuis iSCSI en utilisant l'adaptateur logiciel iSCSI, l'adaptateur est activé et la configuration du réseau est créée automatiquement au premier démarrage. Si vous désactivez l'adaptateur, il est réactivé à chaque démarrage de l'hôte.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez un serveur dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Adaptateurs de stockage]** dans le panneau Matériel.

  La liste des adaptateurs de stockage disponibles apparaît.

3 Sélectionnez l'initiateur iSCSI à configurer et cliquez sur **[Propriétés]** .

4 Cliquez sur **[Configurer]** .

5 Pour activer l'initiateur, sélectionnez **[Activé]** et cliquez sur **[OK]** .

Après l'activation de l'initiateur, l'hôte lui assigne un nom iSCSI par défaut. Vous pouvez modifier le nom par défaut si nécessaire.

Installation et configuration d'adaptateurs iSCSI matériels dépendants

Un adaptateur iSCSI matériel dépendant est un adaptateur tiers qui dépend du réseau VMware et des interfaces de configuration et de gestion iSCSI fournies par VMware.

Ce type d'adaptateur peut être une carte, par exemple Broadcom 5709 NIC, qui fournit un adaptateur réseau standard et la fonctionnalité de déchargement iSCSI pour le même port. La fonctionnalité de déchargement iSCSI apparaît dans la liste des adaptateurs de stockage en tant qu'adaptateur iSCSI. Bien que l'adaptateur iSCSI soit activé par défaut, pour le rendre fonctionnel, vous devez configurer la mise en réseau pour le trafic iSCSI et lier l'adapateur et un port iSCSI VMkernel iSCSI approprié. Vous pourrez alors configurer l'adaptateur.

La procédure complète d'installation et de configuration des adaptateurs iSCSI matériel dépendant comprend les étapes suivantes :

1 Affichez les adaptateurs matériels dépendants.

  Reportez-vous à « Affichage des adaptateurs de matériel iSCSI dépendants », page 106.

  Si vos adaptateurs matériels dépendants n'apparaissent pas dans la liste des adaptateurs de stockage, vérifiez s'ils nécessitent une licence. Consultez la documentation du fabricant.

2 Déterminez l'association entre les adaptateurs matériels dépendants et les NIC physiques.

  Reportez-vous à la section « Détermine l'association entre les adaptateurs de matériel iSCSI dépendants et les adaptateurs réseau physiques », page 106

  Notez bien les noms des NIC physiques correspondants. Par exemple, l'adaptateur vmhba33 correspond au vmnic1 tandis que vmhba34 correspond au vmnic2.

3 Configurez le réseau iSCSI en créant des ports pour le trafic iSCSI.

  Reportez-vous à « Configuration du réseau pour l'iSCSI logiciel et l'iSCSI matériel dépendant », page 75.

  Ouvrez un port pour chaque NIC. Par exemple, créez le port vmk1 pour le vmnic1, et le port vmk2 pour le vmnic2.

4 Associez les ports iSCSI aux adaptateurs iSCSI matériels dépendants correspondants. Cette étape est nécessaire, que vous disposiez de plusieurs adaptateurs ou d'un seul.

  Reportez-vous à « Associer des ports iSCSI aux adaptateurs iSCSI », page 107.

  Dans cet exemple, le port vmk1 est associé à vmhba33, et le port vmk2 est associé à vmbh34.

5 Configurez les adresses de découverte.

  Reportez-vous à « Configurer des adresses de découverte pour des initiateurs iSCSI », page 108.

6 Configurez les paramètres CHAP.

  Reportez-vous à « Configurer des paramètres CHAP pour des cartes iSCSI », page 109.

Considérations sur l'iSCSI matériel dépendant

Lorsque vous utilisez des adaptateurs iSCSI matériels dépendants avec ESX, certaines considérations s'appliquent.

- Lorsque vous utilisez un adaptateur iSCSI matériel dépendant, le rapport de performances pour une carte réseau associée à l'adaptateur ne montre que peu ou pas d'activité, même lorsque le trafic iSCSI est intense. Cela est dû au contournement de la pile réseau habituelle par le trafic iSCSI.
- L'adaptateur iSCSI Broadcom réassemble les données dans le matériel, dont l'espace tampon est limité. Lorsque vous utilisez l'adaptateur iSCSI Broadcom dans un réseau congestionné ou sous chargement, activez le contrôle de flux pour éviter la dégradation des performances.

Le contrôle de flux gère la vitesse de transmission des données entre deux nœuds pour éviter qu'un expéditeur rapide ne dépasse un récepteur lent. Pour obtenir de meilleurs résultats, activez le contrôle du flux aux points d'extrémité du chemin E/S, au niveau des hôtes et des systèmes de stockage iSCSI.

- Les adaptateurs iSCSI Broadcom ne prennent pas en charge les trames IPv6 et les trames jumbo.

Affichage des adaptateurs de matériel iSCSI dépendants

Affichez un adaptateur iSCSI matériel dépendant pour vérifier qu'il est correctement chargé.

Si l'adaptateur matériel dépendant ne figure pas dans la liste des adaptateurs de stockage, vérifiez s'il a besoin d'une licence. Consultez la documentation du fabricant.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez un hôte dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Adaptateurs de stockage]** dans le panneau Matériel.

S'il est installé, l'adaptateur de matériel iSCSI doit figurer dans la liste d'adaptateurs de stockage.

3 Sélectionnez l'adaptateur à afficher et cliquez sur **[Propriétés]** .

La boîte de dialogue Propriétés affiche les détails par défaut pour l'adaptateur, y compris le nom iSCSI et l'alias iSCSI.

Détermine l'association entre les adaptateurs de matériel iSCSI dépendants et les adaptateurs réseau physiques

Vous devez déterminer le nom de la carte réseau physique à laquelle l'adaptateur iSCSI matériel dépendant est associé. Vous devez connaître l'association pour pouvoir effectuer correctement la liaison de port.

Procédure

1 Utilisez la commande vSphere CLI pour déterminer le nom de la carte réseau physique à laquelle l'adaptateur iSCSI est associé.

```
esxcli swiscsi vmnic list –d vmhba#
```

vmhba# est le nom de l'adaptateur iSCSI.

2 Dans la sortie, trouvez la ligne `vmnic name: vmnic#`.

vmnic# est le nom de la carte réseau qui correspond à l'adaptateur iSCSI.

Suivant

Après avoir déterminé le nom de la carte réseau, vous devez créer un port iSCSI sur un vSwitch connecté à la carte. Vous associez alors ce port à l'adaptateur iSCSI matériel dépendant afin que votre hôte puisse diriger le trafic iSCSI via la carte.

Associer des ports iSCSI aux adaptateurs iSCSI

Associez un port iSCSI que vous avez créé pour une carte réseau à un adaptateur iSCSI. En cas d'adaptateur iSCSI logiciel, n'effectuez cette tâche que si vous avez installé deux ou plusieurs NIC pour le multichemin iSCSI. Si vous utilisez des adaptateurs iSCSI matériels dépendants, cette tâche est indispensable que vous ayez un seul ou plusieurs adaptateurs.

Prérequis

Effectuez les tâches suivantes :

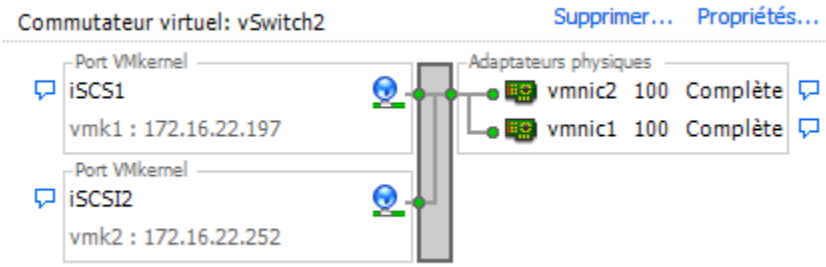
- Pour les adaptateurs iSCSI matériels dépendants, associez correctement les NIC physiques et les adaptateurs iSCSI. Reportez-vous à « Affichage des adaptateurs de matériel iSCSI dépendants », page 106.
- Configurez le réseau pour le trafic iSCSI. Reportez-vous à « Configuration du réseau pour l'iSCSI logiciel et l'iSCSI matériel dépendant », page 75.
- Pour utiliser l'adaptateur logiciel iSCSI, vous devez l'activer. Reportez-vous à « Activer l'adaptateur iSCSI logiciel », page 104.

Procédure

1 Trouvez le nom du port iSCSI assigné au NIC physique.

vSphere Client affiche le nom du port sous l'étiquette de réseau.

Dans le graphique suivant, les noms des ports sont vmk1 et vmk2.



2 Utilisez la commande vSphere CLI pour associer le port iSCSI à l'adaptateur iSCSI.

```
esxcli swiscsi nic add -n port_name -d vmhba
```

IMPORTANT En cas d'iSCSI logiciel, répétez cette commande pour chaque port iSCSI, en connectant tous les ports avec l'adaptateur iSCSI logiciel. En cas d'iSCSI matériel dépendant, assurez-vous d'associer chaque port à un adaptateur correspondant approprié.

3 Vérifiez que le port a été ajouté à l'adaptateur iSCSI.

```
esxcli swiscsi nic list -d vmhba
```

4 Utilisez le vSphere Client pour analyser à nouveau l'adaptateur iSCSI.

Configurer des adresses de découverte pour des initiateurs iSCSI

Configurez les adresses de découverte de cible de sorte que l'initiateur iSCSI puisse déterminer quelle ressource de stockage présente sur le réseau est disponible pour accès.

Le système ESX admet les méthodes de découverte suivantes :

Découverte dynamique Également appelée découverte SendTargets. Chaque fois que l'initiateur contacte un serveur iSCSI désigné, il envoie la demande de SendTargets au serveur. Le serveur répond en fournissant une liste de cibles disponibles à l'initiateur. Les noms et adresses IP de ces cibles figurent dans l'onglet **[Découverte statique]** . Si vous supprimez une cible statique ajoutée par la découverte dynamique, il se peut qu'elle soit réintégrée à la liste la prochaine fois qu'un scannage se produira, que le HBA se réinitialisera ou que l'hôte sera redémarré.

Découverte statique L'initiateur n'a aucune découverte à effectuer. L'initiateur dispose d'une liste de cibles qu'il peut contacter, et emploie leurs adresses IP et noms de cible pour communiquer avec elles.

Configurer la découverte dynamique

Avec la découverte dynamique, chaque fois que l'initiateur contacte un serveur iSCSI précis, il lui envoie la demande SendTargets. Le serveur répond en fournissant une liste de cibles disponibles à l'initiateur.

Quand vous configurez la découverte dynamique, vous pouvez seulement ajouter un nouveau serveur iSCSI. Vous ne pouvez changer l'adresse IP, le nom DNS ni le numéro de port d'un serveur iSCSI existant. Pour apporter des modifications, supprimez le serveur existant et ajoutez-en un nouveau.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez un serveur dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Adaptateurs de stockage]** dans le panneau Matériel.

La liste des adaptateurs de stockage disponibles apparaît.

3 Sélectionnez l'initiateur iSCSI à configurer et cliquez sur **[Propriétés]** .

4 Dans la boîte de dialogue de propriétés d'initiateur iSCSI, cliquez sur l'onglet **[Découverte dynamique]** .

5 Pour ajouter une adresse à la découverte SendTargets, cliquez sur **[Ajouter]** .

La boîte de dialogue **[Ajouter serveur SendTargets]** apparaît.

6 Tapez l'adresse IP ou le nom DNS du système de stockage et cliquez sur **[OK]** .

Dès que votre hôte établit la connexion SendTargets avec ce système, toutes les cibles nouvellement découvertes apparaissent dans la liste Découverte statique.

7 Pour supprimer un serveur SendTargets précis, sélectionnez-le et cliquez sur **[Supprimer]** .

Une fois un serveur SendTargets supprimé, il se peut qu'il apparaisse encore dans le champ Héritage en tant que parent de cibles statiques. Cette entrée, qui signale où les cibles statiques ont été découvertes, n'affecte pas la fonctionnalité.

Suivant

Une fois la découverte dynamique configurée pour votre adaptateur iSCSI, Réanalysez l'adaptateur.

Configurer la découverte statique

Avec les initiateurs iSCSI, outre la méthode de découverte dynamique, vous pouvez utiliser la découverte statique et saisir manuellement des information pour les cibles.

Quand vous configurez la découverte statique, vous pouvez seulement ajouter des cibles iSCSI. Vous ne pouvez changer l'adresse IP, le nom DNS, le nom de cible iSCSI ni le numéro de port d'une cible existante. Pour apporter des modifications, supprimez la cible existante et ajoutez-en une nouvelle.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez un serveur dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Adaptateurs de stockage]** dans le panneau Matériel.

La liste des adaptateurs de stockage disponibles apparaît.

3 Sélectionnez l'initiateur iSCSI à configurer et cliquez sur **[Propriétés]** .

4 Dans la boîte de dialogue de propriétés d'initiateur iSCSI, cliquez sur l'onglet **[Découverte statique]** .

L'onglet affiche toutes les cibles découvertes dynamiquement et toutes les cibles statiques déjà saisies.

5 Pour ajouter une cible, cliquez sur **[Ajouter]** et saisissez les informations sur la cible.

6 Pour supprimer une cible précise, sélectionnez-la et cliquez sur **[Supprimer]** .

Suivant

Une fois la découverte statique configurée pour votre adaptateur iSCSI, Réanalysez l'adaptateur.

Configurer des paramètres CHAP pour des cartes iSCSI

Etant donné que les réseaux IP qu'utilise la technologie iSCSI pour se connecter aux cibles distantes ne protègent pas les données qu'ils transportent, vous devez sécuriser la connexion. L'un des protocoles que l'iSCSI applique est le protocole CHAP, qui vérifie la légitimité des initiateurs qui accèdent à des cibles sur le réseau.

Le protocole CHAP applique un algorithme de négociation à trois voies pour vérifier l'identité de votre hôte et, le cas échéant, de la cible iSCSI quand l'hôte et la cible établissent une connexion. La vérification repose sur une valeur privée prédéfinie, dite secret CHAP, que l'initiateur et la cible partagent.

ESX permet l'authentification CHAP au niveau adaptateur. Dans ce cas, toutes les cibles reçoivent les mêmes nom et secret CHAP de la part de l'initiateur iSCSI. Pour les adaptateurs iSCSI logiciels et matériels dépendants, ESX admet également l'authentification CHAP cible par cible, qui permet de configurer différentes informations d'identification pour chaque cible afin de parvenir à un niveau de sécurité plus élevé.

Choisir la méthode d'authentification CHAP

ESX permet le CHAP unilatéral pour tous les types d'initiateurs iSCSI, et le CHAP mutuel pour l'iSCSI logiciel et matérielle dépendante.

Avant de configurer CHAP, vérifiez s'il est activé dans le système de stockage iSCSI et vérifiez la méthode d'authentification CHAP que le système permet. Si CHAP est activé, activez-le pour vos initiateurs, en veillant à ce que les informations d'identification d'authentification CHAP concordent avec celles du stockage iSCSI.

ESX permet les méthodes d'authentification CHAP suivantes :

CHAP unilatéral En authentification CHAP unilatérale, également appelée unidirectionnelle, la cible authentifie l'initiateur, mais l'initiateur n'authentifie pas la cible.

CHAP mutuel En authentification CHAP mutuelle, également appelée bidirectionnelle, un niveau de sécurité supplémentaire permet à l'initiateur d'authentifier la cible. VMware ne permet cette méthode que pour les cartes iSCSI logiciels et matérielles dépendantes.

Pour les cartes iSCSI logiciels et matérielles dépendantes, vous pouvez définir le CHAP unilatéral et le CHAP mutuel pour chaque initiateur ou au niveau cible. L'iSCSI matérielle ne permet le CHAP qu'au niveau initiateur.

Quand vous définissez les paramètres CHAP, indiquez un niveau de sécurité pour CHAP.

Remarque Quand vous indiquez le niveau de sécurité CHAP, le type de réponse de la baie de stockage dépend de l'implémentation CHAP de la baie et de l'éditeur. Par exemple, si vous cochez `Utiliser CHAP sauf si la cible l'interdit`, certaines baies de stockage appliquent CHAP dans la réponse, alors que d'autres non. Pour plus d'informations sur le comportement de l'authentification CHAP dans différentes configurations d'initiateur et de cible, consultez la documentation de la baie.

Tableau 8-1. Niveau de sécurité CHAP

Niveau de sécurité CHAP	Description	Pris en charge
Ne pas utiliser CHAP	L'hôte n'applique pas l'authentification CHAP. Cochez cette option pour mettre hors tension l'authentification si elle est actuellement activée.	iSCSI logiciel Matériel iSCSI dépendant Matériel iSCSI indépendant
Ne pas utiliser CHAP sauf si la cible l'exige	L'hôte préfère une connexion non CHAP, mais peut utiliser une connexion CHAP si la cible l'exige.	iSCSI logiciel Matériel iSCSI dépendant
Utiliser CHAP sauf si la cible l'interdit	L'hôte préfère CHAP, mais peut utiliser des connexions non CHAP si la cible ne gère pas CHAP.	iSCSI logiciel Matériel iSCSI dépendant Matériel iSCSI indépendant
Utiliser CHAP	L'hôte exige une authentification CHAP réussie. La connexion échoue si la négociation CHAP échoue.	iSCSI logiciel Matériel iSCSI dépendant

Configurer les informations d'identification CHAP pour un initiateur iSCSI

Vous pouvez configurer toutes les cibles pour qu'elles reçoivent les mêmes nom et secret CHAP de l'initiateur iSCSI au niveau de l'initiateur. Par défaut, toutes les adresses de découverte ou cibles statiques héritent des paramètres CHAP que vous configurez au niveau initiateur.

Prérequis

Avant de configurer des paramètres CHAP pour l'iSCSI logiciel ou matérielle dépendante, déterminez s'il faut configurer un CHAP unilatéral ou mutuel. Les adaptateurs iSCSI matériels indépendants n'admettent pas le CHAP mutuel.

- En CHAP unilatéral, la cible authentifie l'initiateur.
- En CHAP mutuel, la cible et l'initiateur s'authentifient réciproquement. Veillez à utiliser différents secrets pour le CHAP et le CHAP mutuel.

Quand vous configurez des paramètres CHAP, assurez-vous qu'ils concordent avec les paramètres du côté stockage.

Le nom CHAP ne doit pas excéder 511 et le mot de passe CHAP 255 caractères alphanumériques. Certains adaptateurs, par exemple l'adaptateur QLogic, peuvent avoir des limites plus basses, 255 pour le nom CHAP et 100 pour le secret CHAP.

Procédure

1 Accédez à la boîte de dialogue de propriétés d'initiateur iSCSI.

2 Dans l'onglet **[Général]** , cliquez sur **[CHAP]** .

3 Pour configurer le CHAP unilatéral, sous CHAP, spécifiez ce qui suit :

   a Sélectionnez le niveau de sécurité CHAP.

      - **[Utilisez CHAP juste si cible le demande]** (iSCSI logiciel et matérielle dépendante uniquement)
      - **[Utiliser CHAP sauf si interdit par la cible]**
      - **[Utiliser CHAP]** (iSCSI logiciel et matérielle dépendante uniquement) Pour pouvoir configurer le CHAP mutuel, vous devez sélection cette option.

   b Indiquez le nom CHAP.

      Assurez-vous que le nom que vous indiquez concorde avec celui configuré côté stockage.

      - Pour désigner comme nom CHAP le nom d'initiateur iSCSI, cochez **[Utiliser nom initiateur]** .
      - Pour désigner comme nom CHAP toute autre chose que le nom d'initiateur iSCSI, décochez **[Utiliser nom initiateur]** et tapez un nom dans le champ **[Nom]** .

   c Saisissez un secret CHAP unilatéral à utiliser dans le cadre de l'authentification. Veillez à utiliser le même secret que celui que vous saisissez côté stockage.

4 Pour configurer le CHAP mutuel, configurez d'abord le CHAP unilatéral selon les instructions de Étape 3

   Veillez à cocher **[Utiliser CHAP]** comme option du CHAP unilatéral. Ensuite, spécifiez les paramètres suivants sous **[CHAP mutuel]** :

   a Cochez **[Utiliser CHAP]** .

   b Indiquez le nom CHAP mutuel.

   c Tapez le secret CHAP mutuel. Veillez à utiliser des secrets différents pour le CHAP unilatéral et le CHAP mutuel.

5 Cliquez sur **[OK]** .

6 Réanalysez l'initiateur.

Si vous modifiez les paramètres CHAP ou CHAP mutuel, ils sont appliqués aux nouvelles sessions iSCSI. Pour les sessions existantes, les nouveaux paramètres ne sont appliqués qu'une fois que vous vous êtes déconnecté puis reconnecté.

Configurer les informations d'identification CHAP pour une cible

Pour les cartes iSCSI matérielles qui dépendent du logiciel, vous pouvez définir des informations d'identification CHAP différentes pour chaque adresse de découverte ou cible statique.

Quand vous configurez des paramètres CHAP, assurez-vous qu'ils concordent avec les paramètres du côté stockage. Le nom CHAP ne doit pas excéder 511 et le secret CHAP ne doit pas excéder 255 caractères alphanumériques.

Prérequis

Avant de configurer des paramètres CHAP pour l'iSCSI logiciel et matérielle dépendante, déterminez s'il faut configurer un CHAP unilatéral ou mutuel.

- En CHAP unilatéral, la cible authentifie l'initiateur.
- En CHAP mutuel, la cible et l'initiateur s'authentifient réciproquement. Veillez à utiliser différents secrets pour le CHAP et le CHAP mutuel.

Procédure

1 Accédez à la boîte de dialogue de propriétés d'initiateur iSCSI.

2 Sélectionnez soit l'onglet **[Découverte dynamique]** , soit l'onglet **[Découverte statique]** .

3 Dans la liste de cibles disponibles, sélectionnez la cible que vous voulez configurer et cliquez sur **[Paramètres]** > **[CHAP]** .

4 Configurez le CHAP unilatéral dans la zone CHAP.

   a Décochez **[Hériter du parent]** .

   b Sélectionnez l'une des options suivantes :

   - **[Ne pas utiliser CHAP sauf si la cible l'exige]**
   - **[Utiliser CHAP sauf si la cible l'interdit]**
   - **[Utiliser CHAP]** . Pour pouvoir configurer le CHAP mutuel, vous devez sélection cette option.

   c Indiquez le nom CHAP.

   Assurez-vous que le nom que vous indiquez concorde avec celui configuré côté stockage.

   - Pour désigner comme nom CHAP le nom d'initiateur iSCSI, cochez **[Utiliser nom initiateur]** .
   - Pour désigner comme nom CHAP toute autre chose que le nom d'initiateur iSCSI, décochez **[Utiliser nom initiateur]** et tapez un nom dans le champ **[Nom]** .

   d Saisissez un secret CHAP unilatéral à utiliser dans le cadre de l'authentification. Veillez à utiliser le même secret que celui que vous saisissez côté stockage.

5 Pour configurer le CHAP mutuel, configurez d'abord le CHAP unilatéral selon les instructions de Étape 4.

   Veillez à cocher **[Utiliser CHAP]** comme option du CHAP unilatéral. Ensuite, spécifiez les paramètres suivants dans la zone Mutual CHAP :

   a Décochez **[Hériter du parent]** .

   b Cochez **[Utiliser CHAP]** .

   c Indiquez le nom CHAP mutuel.

   d Tapez le secret CHAP mutuel. Veillez à utiliser des secrets différents pour le CHAP unilatéral et le CHAP mutuel.

6 Cliquez sur **[OK]** .

7 Réanalysez l'initiateur.

Si vous modifiez les paramètres CHAP ou CHAP mutuel, ils sont appliqués aux nouvelles sessions iSCSI. Pour les sessions existantes, les nouveaux paramètres ne sont appliqués qu'une fois que vous vous êtes déconnecté puis reconnecté.

Désactiver CHAP

Vous pouvez mettre hors tension le protocole CHAP si le système de stockage ne le nécessite pas.

Si vous désactivez CHAP sur un système qui exige l'authentification CHAP, les sessions iSCSI existantes demeurent actives jusqu'à ce que vous redémarriez votre hôte ESX ou que le système de stockage oblige à se déconnecter. Une fois la session close, vous ne pouvez plus vous connecter aux cibles qui exigent CHAP.

Procédure

1 Ouvrez la boîte de dialogue d'informations d'identification CHAP.

2 Avec les adaptateurs iSCSI logiciels et matériels dépendants, pour ne mettre hors tension que le CHAP mutuel et laisser le CHAP unilatéral, cochez **[Ne pas utiliser le CHAP]** dans la zone CHAP mutuel.

3 Pour mettre hors tension le CHAP unilatéral, cochez **[Ne pas utiliser le CHAP]** dans la zone CHAP.

Le CHAP mutuel, s'il est installé, passe automatiquement à **[Ne pas utiliser le CHAP]** si vous désactivez le CHAP unilatéral.

4 Cliquez sur **[OK]** .

Configurer des paramètres supplémentaires pour l'iSCSI

Il se peut que vous deviez configurer des paramètres supplémentaires pour vos initiateurs iSCSI. Par exemple, certains systèmes de stockage iSCSI exigent la redirection ARP (Address Resolution Protocol) pour mouvoir le trafic iSCSI dynamiquement d'un port à l'autre. Dans ce cas, vous devez activer la redirection ARP sur votre hôte.

Tableau 8-2 répertorie les paramètres iSCSI avancés que vous pouvez configurer au moyen de vSphere Client. En outre, vous pouvez utiliser la commande vSphere CLI `vicfg-vicfg-iscsi` pour configurer certains des paramètres avancés. Pour en savoir plus, reportez-vous à *Guide d'installation et script de l'interface de ligne de commande vSphere et Référence de l'interface de ligne de commande vSphere*.

N'apportez aucune modification aux paramètres iSCSI avancés à moins de travailler avec l'équipe d'assistance VMware ou de disposer par d'autres biais d'informations précises sur les valeurs à attribuer aux paramètres.

Tableau 8-2. Paramètres supplémentaires des initiateurs iSCSI

Paramètre avancé	Description	Configurable sur
Résumé d'en-tête	Augmente l'intégrité des données. Si le prétraitement d'en-tête est activé, le système effectue un total de contrôle sur la partie d'en-tête de chaque unité de données de protocole (PDU) iSCSI et le vérifie au moyen de l'algorithme CRC32C.	iSCSI logiciel Matériel iSCSI dépendant
Résumé de données	Augmente l'intégrité des données. Si le résumé de données est activé, le système effectue un total de contrôle sur la partie données de chaque unité de données de protocole (PDU) et le vérifie au moyen de l'algorithme CRC32C. **Remarque** Les systèmes qui utilisent des processeurs Intel Nehalem délestent les calculs de résumé iSCSI pour l'iSCSI logiciel, en réduisant ainsi l'incidence sur les performances.	iSCSI logiciel Matériel iSCSI dépendant
Maximum Outstanding R2T (Maximum d'unités de données de protocole en suspend prêtes à envoyer)	Définit le nombre d'unités de données de protocole (PDU) prêtes à envoyer qui peut être en transition avant qu'une PDU d'accusé de réception ne soit reçue.	iSCSI logiciel Matériel iSCSI dépendant
First Burst Length (Longueur de première salve)	Indique la quantité maximum de données non sollicitées qu'un initiateur iSCSI peut envoyer à la cible pendant l'exécution d'une commande SCSI, en octets.	iSCSI logiciel Matériel iSCSI dépendant
Maximum Burst Length (Longueur maximum de salve)	Charge utile de données maximum dans une séquence iSCSI d'entrée de données ou de sortie de données sollicitée, en octets.	iSCSI logiciel Matériel iSCSI dépendant
Maximum Receive Data Segment Length (Longueur maximum de segment de données en réception)	Longueur maximum de segment de données, en octets, qui peut être reçu dans une PDU iSCSI.	iSCSI logiciel Matériel iSCSI indépendant

Tableau 8-2. Paramètres supplémentaires des initiateurs iSCSI (suite)

Paramètre avancé	Description	Configurable sur
Session Recovery Timeout (Délai de récupération de session)	Indique le laps de temps, en secondes, qui peut s'écouler pendant que s'exécute une récupération de session. Si le délai dépasse sa limite, l'initiateur iSCSI termine la session.	iSCSI logiciel Matériel iSCSI dépendant
No-Op Interval (Intervalle sans opération)	Indique l'intervalle, en secondes, entre les demandes en sortie sans opération envoyées par votre initiateur iSCSI à une cible iSCSI. Les demandes en sortie sans opération servent de mécanisme ping pour vérifier qu'une connexion entre l'initiateur iSCSI et la cible iSCSI est active.	iSCSI logiciel Matériel iSCSI dépendant
No-Op Timeout (Délai de demande sans opération)	Indique le laps de temps, en secondes, qui peut s'écouler avant que votre hôte ne reçoive un message d'entrée sans opération (NOP-In). Le message est envoyé par la cible iSCSI en réponse à la demande en sortie sans opération. Dès que la limite de délai sans opération est dépassée, l'initiateur clôt la session actuelle et en démarre une nouvelle.	iSCSI logiciel Matériel iSCSI dépendant
ARP Redirect (Redirection ARP)	Permet aux systèmes de stockage de mouvoir le trafic iSCSI dynamiquement d'un port à l'autre. L'ARP est exigé par les systèmes de stockage qui appliquent le basculement basé sur baie.	iSCSI logiciel et matériel indépendant (Configurable via vSphere CLI)
Accusé de réception retardé	Permet aux systèmes de retarder l'accusé de réception des paquets de données.	iSCSI logiciel Matériel iSCSI dépendant

Configurer les paramètres avancés d'iSCSI

Les paramètres iSCSI avancés contrôlent des paramètres tels que le résumé de l'en-tête et des données, la redirection ARP, l'accusé de réception différé, etc. Généralement, vous n'avez pas besoin de modifier ces paramètres, car votre hôte ESX fonctionne avec les valeurs prédéfinies.

Avertissement N'apportez aucune modification aux paramètres iSCSI avancés à moins de travailler avec l'équipe d'assistance VMware ou de disposer par d'autres biais d'informations précises sur les valeurs à attribuer aux paramètres.

Procédure

1 Accédez à la boîte de dialogue de propriétés d'initiateur iSCSI.

2 Pour configurer les paramètres avancés au niveau initiateur, dans l'onglet Général, cliquez sur **[Avancé]** . Passez à Étape 4.

3 Configurez les paramètres avancés au niveau cible.

Au niveau cible, les paramètres avancés ne peuvent être configurés que pour les adaptateurs iSCSI logiciels et matériels dépendants.

a Sélectionnez soit l'onglet **[Découverte dynamique]** , soit l'onglet **[Découverte statique]** .

b Dans la liste de cibles disponibles, sélectionnez une cible à configurer et cliquez sur **[Paramètres] > [Avancé]** .

4 Saisissez toute valeur obligatoire des paramètres avancés que vous voulez modifier et cliquez sur **[OK]** pour enregistrer vos modifications.

Actualisation de la banque de données et opérations de réanalyse du stockage

L'opération d'actualisation de la banque de données met à niveau les listes de la banque de données et les informations de stockage, comme la capacité de la banque de données, affichées dans vSphere Client. Lorsque vous effectuez des tâches de gestion de la banque de données ou que vous modifiez la configuration SAN, il se peut que vous deviez réanalyser le stockage.

Lorsque vous effectuez des opérations de gestion de la banque de données VMFS, comme la création d'une banque de données VMFS ou d'un RDM, l'ajout d'une extension et l'augmentation ou la suppression d'une banque de données VMFS, votre hôte ou le vCenter Server réanalyse automatiquement le stockage et le met à niveau. Vous pouvez mettre hors tension la fonction de réanalyse automatique en désactivant le filtre de réanalyse de l'hôte. Reportez-vous à « Désactiver les filtres de stockage vCenter Server », page 140.

Dans certains cas, vous devez effectuer une réanalyse manuel. Vous pouvez réanalyser tous les stockages disponibles sur votre hôte ou, si vous utilisez le vCenter Server, sur tous les hôtes d'un dossier, d'un cluster et d'un centre de données.

Si les modifications que vous apportez ne concernent que le stockage connecté à un adapteur spécifique, effectuez une réanalyse pour cette carte.

Effectuez la réanalyse manuelle chaque fois que vous apportez les modifications suivantes.

- Création de nouveaux LUN sur un SAN.
- Modification du masquage de chemin sur un hôte.
- Reconnecter un câble
- Modification des paramètres CHAP
- Ajout d'un seul hôte dans le vCenter Server après la modification ou la suppression du vCenter Server d'une banque de données partagée par les hôtes du vCenter Server et un seul hôte.

IMPORTANT Si vous réanalysez quand un chemin n'est pas disponible, l'hôte le supprime de la liste de chemins sur le périphérique. Ce chemin réapparaît dans la liste dès qu'il devient disponible et recommence à fonctionner.

Rescanner le stockage

Lorsque vous apportez des modifications à la configuration de votre SAN, vous pouvez avoir besoin de réanalyser votre stockage. Vous pouvez réanalyser tout le stockage disponible de votre hôte. Si les modifications que vous apportez ne concernent que le stockage accessible par un adaptateur spécifique, effectuez une réanalyse seulement pour cet adaptateur.

Appliquez cette procédure si vous voulez limiter la réanalyse au stockage disponible pour un hôte particulier ou un hôte auquel on accède par un adaptateur particulier. Si vous voulez réanalyser le stockage disponible à tous les hôtes gérés par votre système vCenter Server, vous pouvez le faire en cliquant avec le bouton droit sur un centre de données, un cluster ou un dossier qui contient les hôtes et en sélectionnant **[réanalyse banques de données]** .

Procédure

1 Dans vSphere Client, sélectionnez un hôte et cliquez sur l'onglet **[Configuration]** .

2 Dans le panneau Matériel, sélectionnez **[Adaptateurs de stockage]** , et cliquez sur **[réanalyse]** au-dessus du panneau Adaptateurs de stockage.

Vous pouvez également cliquer avec le bouton droit sur un adaptateur individuel et cliquer sur **[Réanalyser]** pour ne réanalyser que cet adaptateur.

3 Pour détecter les nouveaux disques ou LUN, cochez **[Analyser nouveau périphérique stockage]** .

Si de nouveaux LUN sont découverts, ils apparaissent dans la liste de périphériques.

4 Pour détecter les nouvelles banque de données ou mettre à niveau une banque de données après que sa configuration a été modifiée, cochez **[Analyser nouveaux volumes VMFS]** .

Si de nouvelles banques de données ou de nouveaux volumes VMFS sont découverts, ils apparaissent dans la liste de banque de données.

Créer des banques de données VMFS

Les banques de données VMFS servent de référentiel aux machines virtuelles. Vous pouvez configurer des banque de données VMFS sur des périphériques de stockage SCSI que l'hôte trouve.

Prérequis

Avant de créer des banques de données, vous devez installer et configurer toutes les cartes dont votre stockage a besoin. Réanalysez les cartes pour détecter les périphériques de stockage nouvellement ajoutés.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Stockage]** dans le panneau Matériel.

3 Cliquez sur **[banque de données]** et cliquez sur **[Ajouter stockage]** .

4 Sélectionnez le type de stockage **[Disque/LUN]** et cliquez sur **[Suivant]** .

5 Sélectionnez un périphérique à utiliser pour votre banque de données et cliquez sur **[Suivant]** .

REMARQUE Sélectionnez le périphérique sans nom de banque de données affiché dans la colonne VMFS Label. Si un nom est présent, le périphérique contient une copie d'une banque de données VMFS existante.

Si le disque que vous formatez est vierge, la page Disposition actuelle du disque présente automatiquement l'espace disque entier pour la configuration du stockage.

6 Si le disque n'est pas vierge, passez en revue la disposition actuelle de disque dans le panneau supérieur de la page Disposition actuelle du disque et sélectionnez une option de configuration dans le panneau inférieur.

Option	Description
Utilisez toutes les partitions disponibles	Réserve le disque ou LUN entier à une seule banque de données VMFS. Si vous sélectionnez cette option, tous les systèmes de fichiers et données actuellement stockés sur ce périphérique sont détruits.
Utilisez l'espace libre	Déploie une banque de données VMFS dans l'espace libre restant du disque.

7 Cliquez sur **[Suivant]** .

8 Dans la page Propriétés, entrez le nom d'une banque de données et cliquez sur **[Suivant]** .

9 Si nécessaire, ajustez le système de fichiers et les valeurs de capacité.

Par défaut, l'espace libre entier sur le périphérique de stockage est disponible.

10 Cliquez sur **[Suivant]** .

11 Sur la page Prêt à Terminer, passez en revue les informations de configuration de banque de données et cliquez sur **[Terminer]** .

Une banque de données sur le périphérique de stockage SCSI est créée. Si vous employez le système vCenter Server pour gérer vos hôtes, la banque de données nouvellement créée est automatiquement ajoutée à tous les hôtes.

Stockage relié au réseau (NAS)

ESX prend en charge l'utilisation de NAS via le protocole NFS. Le protocole NFS permet la communication entre un client NFS et un serveur NFS.

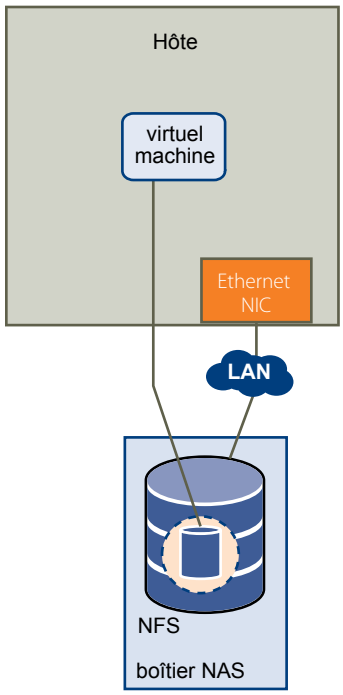
Le client NFS intégré dans ESX vous laisse accéder au serveur NFS et utiliser les volumes NFS pour le stockage. ESX prend en charge uniquement NFS Version 3 sur TCP.

Vous utilisez le vSphere Client pour configurer les volumes NFS comme banque de données. Les banque de données NFS configurées apparaissent dans vSphere Client et vous pouvez les utiliser pour stocker des fichiers de disque virtuel de la même manière que vous utilisez les banque de données VMFS.

Remarque ESX ne prend en charge pas la fonctionnalité d'utilisateur délégué qui permet d'accéder aux volumes NFS via des informations d'identification non-racine.

Figure 8-4 décrit une machine virtuelle utilisant le volume NFS pour stocker ses fichiers. Dans cette configuration, l'hôte se connecte au serveur NFS stockant les fichiers du disque virtuel via un adaptateur réseau normale.

Figure 8-4. Stockage NFS



Les disques virtuels que vous créez sur des banque de données NFS utilisent un format de disque dicté par le serveur NFS, généralement un format léger qui requiert un emplacement d'espace à la demande. Si la machine virtuelle manque d'espace au cours de l'écriture sur ce disque, le vSphere Client vous informe de la nécessité de plus d'espace. Vous disposez des options suivantes :

- Libérez de l'espace supplémentaire sur le volume afin que la machine virtuelle puisse continuer à écrire sur le disque.
- Mettez fin à la session de la machine virtuelle. Terminer la session arrête la machine virtuelle.

AVERTISSEMENT Lorsque votre hôte accède au fichier de disque d'une machine virtuelle sur une banque de données NFS, un fichier de verrouillage `.lck-XXX` est généré dans le même répertoire que celui du fichier de disque afin d'empêcher d'autres disques d'accéder à ce fichier de disque virtuel. Ne supprimez pas le fichier de verrouillage `.lck-XXX` car sans lui, la machine virtuelle en cours d'exécution ne peut pas accéder au fichier de disque virtuel.

Banques de données NFS comme référentiels des fichiers couramment utilisés

En plus du stockage des disques virtuels sur des banque de données NFS, vous pouvez employer NFS comme référentiel central pour les images ISO, les modèles de machine virtuelle, etc.

Pour utiliser NFS comme référentiel partagé, vous créez un répertoire sur le serveur NFS et le montez comme banque de données sur tous les hôtes. Si vous utilisez la banque de données pour les images ISO, vous pouvez connecter le périphérique CD-ROM de la machine virtuelle à un fichier ISO sur la banque de données, et installer un système d'exploitation invité depuis le fichier ISO.

REMARQUE Si le volume NFS sous-jacent sur lequel sont stockés les fichiers est en lecture seule, assurez-vous que le volume soit exporté comme partage en lecture seule par le serveur NFS, ou configurez-le comme banque de données en lecture seule sur l'hôte ESX. Sinon, l'hôte considère que la banque de données est en Lecture/Écriture et risque de ne pas pouvoir ouvrir les fichiers.

Créer une banque de données NFS

Vous pouvez employer l'assistant Ajouter stockage pour monter un volume NFS et l'employer comme s'il s'agissait d'une banque de données VMFS.

Prérequis

Puisque NFS impose que la connectivité réseau accède aux données stockées sur les serveurs distants, avant de configurer NFS, vous devez d'abord configurer la mise en réseau VMkernel.

Procédure

1. Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.
2. Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Stockage]** dans le panneau Matériel.
3. Cliquez sur **[banque de données]** et cliquez sur **[Ajouter stockage]** .
4. Sélectionnez **[Système de fichiers réseau]** comme le type de stockage et cliquez sur **[Suivant]** .
5. Entrez le nom du serveur, le nom de dossier du point de montage et le nom de la banque de données.

   REMARQUE Quand vous montez le même volume NFS sur plusieurs hôtes, s'assurer que les noms de serveur et de dossier sont identiques sur les hôtes. Si les noms ne correspondent pas exactement, par exemple si vous entrez **`partage`** comme nom de dossier sur un hôte et **`/partage`** sur l'autre, les hôtes voient le même volume NFS en tant que deux banque de données différentes. Il peut s'ensuivre une défaillance de certaines fonctions comme vMotion.

6 (Facultatif) Sélectionnez **[Montage NFS lecture seule]** si le volume est exporté en Lecture seule par le serveur NFS.

7 Cliquez sur **[Suivant]** .

8 Dans la page Résumé de système de fichiers réseau, passez en revue les options de configuration et cliquez sur **[Finir]** .

Créer une partition de diagnostic

Pour s'exécuter correctement, votre hôte nécessite une partition de diagnostic ou une partition de décharge pour stocker les vidages mémoire destinés au débogage et au support technique. Vous pouvez créer la partition de diagnostic sur un disque local ou sur un LUN de réseau de stockage SAN privé ou partagé.

Une partition de diagnostic ne peut pas être située sur un LUN iSCSI accessible par un initiateur logiciel iSCSI.

Chaque hôte doit avoir une partition de diagnostic de 100 Mo. Si plusieurs hôtes partagent un réseau de stockage SAN, configurez une partition de diagnostic avec 100 Mo pour chaque hôte.

AVERTISSEMENT Si deux hôtes partageant une partition de diagnostic échouent et enregistrent les vidages mémoire au même emplacement, les vidages mémoire risquent d'être perdus. Pour collecter les données de vidage mémoire, redémarrez un hôte et extrayez les fichiers journaux immédiatement après la défaillance de ce dernier. Toutefois, si un autre hôte échoue avant que vous n'ayez pu collecter les données de diagnostic du premier hôte, le second hôte ne parviendra pas à enregistrer le vidage mémoire.

Avec l'hôte ESX, vous créez généralement une partition de diagnostic lors de l'installation d'ESX en sélectionnant **[Partitionnement recommandé]** . Le programme d'installation crée automatiquement une partition de diagnostic pour votre hôte. Si vous sélectionnez **[Partitionnement avancé]** et choisissez de ne pas spécifier la partition de diagnostic pendant l'installation, vous pouvez la configurer en employant l'assistant Ajouter stockage.

Créer une partition de diagnostic

Vous pouvez créer une partition de diagnostic pour votre hôte.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez l'hôte dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Stockage]** dans le panneau Matériel.

3 Cliquez sur **[banque de données]** et cliquez sur **[Ajouter stockage]** .

4 Sélectionnez **[Diagnostic]** et cliquez sur **[Suivant]** .

Si **[Diagnostic]** n'apparaît pas comme option, l'hôte a déjà une partition de diagnostic.

Vous pouvez interroger et analyser la partition de diagnostic de l'hôte en utilisant la commande `vicfg-dumppart -l` sur vSphere CLI.

5 Spécifiez le type de partition de diagnostic.

Option	Description
Local privé	Crée la partition de diagnostic sur un disque local. Cette partition stocke les informations de défaillance uniquement pour votre hôte.
Stockage SAN privé	Crée la partition de diagnostic sur un LUN de réseau de stockage SAN non partagé. Cette partition stocke les informations de défaillance uniquement pour votre hôte.
Stockage SAN partagé	Crée la partition de diagnostic sur un LUN de SAN partagé. Cette partition est accessible par plusieurs hôtes et peut stocker des information de défaillance pour plus d'un hôte.

6 Cliquez sur **[Suivant]** .

7 Sélectionnez le périphérique à utiliser pour la partition de diagnostic et cliquez sur **[Suivant]** .

8 Passez en revue les informations de configuration de la partition et cliquez sur **[Terminer]** .

Gestion du stockage 9

Après avoir créé des banque de données, vous pouvez modifier leurs propriétés, utiliser des dossiers pour regroupesr les banque de données en fonction de vos besoins professionnels ou supprimer les banque de données non utilisées. Vous pouvez également configurer les chemins multiples pour vos copies de banque de données de stockage ou de nouvelle signature.

Ce chapitre aborde les rubriques suivantes :

Gestion des banques de données

Un système ESX utilise les banque de données pour stocker tous les fichiers associés à ses machines virtuelles. Après avoir créé les banque de données, vous pouvez les gérer en réalisant un certain nombre de tâches.

Une banque de données est une unité de stockage logique pouvant utiliser de l'espace disque sur un périphérique physique, une partition de disque ou s'étendre sur plusieurs périphériques physiques. Les banque de données peuvent exister sur différents types de périphériques physiques, y compris SCSI, iSCSI, réseau SAN Fibre Channel ou NFS.

Les banque de données sont ajoutées à vSphere Client de l'une des manières suivantes :

- Reconnaissance en cas d'ajout d'hôte à l'inventaire. vSphere Client affiche les banque de données que l'hôte peut reconnaître.
- Créées sur un périphérique de stockage disponible à l'aide de la commande **[Ajouter stockage]** .

Après avoir créé les banque de données, vous pouvez les employer pour stocker des fichiers de machine virtuelle. Vous pouvez les gérer en les renommant, les supprimant et en définissant des autorisations de contrôle d'accès. Par ailleurs, vous pouvez regroupesr les banque de données afin de les organiser et de définir les mêmes autorisations au sein du groupes simultanément.

Pour plus d'informations sur la définition des autorisations de contrôle d'accès sur une banque de données, voir l'*Aide de vSphere Client*.

Renommage des banques de données

Vous pouvez modifier le nom d'une banque de données existante.

Procédure

1 Affichez les banques de données.

2 Cliquez avec le bouton droit sur la banque de données à renommer et sélectionnez **[Renommer]** .

3 Entrez un nouveau nom de banque de données.

Si vous utilisez le système de vCenter Server pour gérer vos hôtes, le nouveau nom s'affiche sur tous les hôtes qui ont accès à la banque de données.

Regroupesment de banques de données

Si vous utilisez le système vCenter Server pour gérer vos hôtes, regroupesz les banque de données en dossiers. Cette opération permet d'organiser votre banque de données en fonction des pratiques professionnelles et d'affecter des autorisations et des alarmes sur les banque de données d'un groupes simultanément.

Procédure

1 Connectez-vous au vSphere Client Client.

2 Au besoin, affichez les banques de données.

Pour plus d'informations, voir l'aide de vSphere Client.

3 Dans le panneau d'inventaire, choisissez **[banque de données]** .

4 Sélectionnez le centre de données contenant les banques de données à regroupesr.

5 Dans le menu de raccourcis, cliquez sur l'icône **[Nouveau dossier]** .

6 Donnez un nom descriptif au dossier.

7 Cliquez sur chaque banque de données et faites-la glisser dans le dossier.

Suppression des banques de données

Vous pouvez supprimer n'importe quel type de banque de données VMFS, y compris les copies que vous avez montées sans nouvelle signature. Quand vous supprimez une banque de données, elle est détruite et disparaît de tous les hôtes qui y ont accès.

Prérequis

Avant de supprimer une banque de données, retirez toutes les machines virtuelles qui s'y trouvent. Vérifiez qu'aucun autre hôte n'accède à la banque de données.

Procédure

1 Affichez les banques de données.

2 Cliquez avec le bouton droit sur la banque de données à supprimer et sélectionnez **[Supprimer]** .

3 Confirmez que vous voulez supprimer la banque de données.

Démontage des banques de données

Quand vous démontez une banque de données, elle reste intacte, mais ne peut être vue des hôtes que vous spécifiez. Une banque de données démontée continue à s'afficher sur d'autres hôtes, où elle reste montée.

Vous pouvez démonter seulement les types suivants de banques de données :

- banques de données NFS
- Les copies de la banque de données VMFS montées sans resignature

Vous ne pouvez pas démonter une banque de données montée active.

Procédure

1 Affichez les banques de données.

2 Cliquez avec le bouton droit sur la banque de données à démonter et sélectionnez **[Démonter]** .

3 Si la banque de données est partagée, spécifiez quels hôtes ne devraient plus accéder à la banque de données.

   a Si nécessaire, désélectionnez les hôtes où vous souhaitez maintenir votre banque de données montée.

   Par défaut, tous les hôtes sont sélectionnés.

   b Cliquez sur **[Suivant]** .

   c Passez en revue la liste de hôtes desquels vous voulez démonter votre banque de données, et cliquez sur **[Terminer]** .

4 Confirmez que vous voulez démonter la banque de données.

Modification des propriétés de la banque de données VMFS

Après avoir créé une banque de données VMFS, vous pouvez la modifier. Par exemple, vous pouvez l'augmenter si vous avez besoin de plus d'espace. Si vous avez des banque de données VMFS-2, vous pouvez les mettre à niveau au format VMFS-3.

Les banque de données utilisant le format VMFS sont déployées sur des périphériques de stockage SCSI.

Vous ne pouvez pas reformater une banque de données VMFS utilisée par un hôte distant. Si vous essayez, un avertissement apparaît qui précise le nom de la banque de données en cours d'utilisation et l'hôte qui l'utilise. Cet avertissement apparaît également dans les fichiers journaux de VMkernel et vmkwarning.

Selon que votre vSphere Client Client est connecté à un système vCenter Server ou directement à un hôte, vous pouvez accéder à la boîte de dialogue Propriétés banque de données de différentes manières.

- vCenter Server uniquement. Pour accéder à la boîte de dialogue Datastore Properties, sélectionnez la banque de données dans l'inventaire, cliquez sur l'onglet **[Configuration]** , puis sur **[Propriétés]** .
- vCenter Server et hôte ESX. Pour accéder à la boîte de dialogue Datastore Properties, sélectionnez un hôte dans l'inventaire, cliquez sur l'onglet **[Configuration]** , puis sur **[Stockage]** . Dans la vue banque de données, sélectionnez la banque de données à modifier et cliquez sur **[Propriétés]** .

Augmentation des banques de données VMFS

Lorsque vous devez créer de nouvelles machines virtuelles sur une banque de données, ou lorsque les machines virtuelles fonctionnant sur cette banque de données exigent plus d'espace, vous pouvez dynamiquement augmenter la capacité d'une banque de données VMFS.

Sélectionnez l'une des méthodes suivantes :

- Ajoutez une nouvelle extension. Une extension est une partition sur un périphérique de stockage, ou LUN. Vous pouvez ajouter jusqu'à 32 extensions du même type de stockage sur une banque de données VMFS existante. La banque de données VMFS étendue peut utiliser toutes ses extensions à tout moment. Elle ne doit pas nécessairement remplir une extension spécifique avant d'utiliser la suivante.
- Augmentez une extension dans une banque de données VMFS existante, afin qu'elle remplisse la capacité adjacente disponible. Seules les extensions avec de l'espace libre juste après eux sont extensibles.

Remarque Si une banque de données partagée dispose de machines virtuelles activées et est remplie à 100 %, vous pouvez augmenter la capacité de celle-ci uniquement à partir de l'hôte, auprès duquel les machines virtuelles activées sont enregistrées.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez un hôte dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Stockage]** .

3 Dans la vue banque de données, sélectionnez la banque de données à augmenter et cliquez sur **[Propriétés]** .

4 Cliquez sur **[Augmenter]** .

5 Sélectionnez un périphérique de la liste des périphériques de stockage et cliquez sur **[Suivant]** .

   - Si vous voulez ajouter une nouvelle extension, sélectionnez le périphérique pour lequel la colonne Extensible indique Non.
   - Si vous voulez agrandir une extension existante, sélectionnez le périphérique pour lequel la colonne Extensible indique Yes.

6 Sélectionnez une option de configuration dans le panneau du bas.

   Selon la disposition actuelle du disque et vos sélections précédentes, les options que vous voyez pourraient varier.

Option	Description
Utilisez l'espace libre pour ajouter la nouvelle extension	Ajoute de l'espace libre sur ce disque comme nouvelle extension de la banque de données.
Utilisez l'espace libre pour élargir l'extension existante	Augmente une extension existante à la capacité requise.
Utilisez l'espace libre	Déploie une extension dans l'espace libre restant du disque. Cette option est disponible seulement en ajoutant une extension.
Utilisez toutes les partitions disponibles	Dédie le disque entier à une extension unique de la banque de données. Cette option est disponible seulement lors de l'ajout d'une extension et si le disque que vous formatez n'est pas vide. Le disque est reformaté et les banque de données et toutes les données qu'elles contiennent sont effacées.

7 Définissez la capacité de l'extension.

   Par défaut, l'espace libre entier sur le périphérique de stockage est disponible.

8 Cliquez sur **[Suivant]** .

9 Passez en revue la disposition proposée et la nouvelle configuration de votre banque de données et cliquez sur **[Terminer]** .

Suivant

Après avoir augmenté une extension dans une banque de données VMFS partagée, actualisez la banque de données sur chaque hôte pouvant y accéder afin que vSphere Client puisse afficher la capacité correcte de la banque de données pour tous les hôtes.

Mettre à niveau les banques de données

ESX comprend VMFS version 3 (VMFS-3). Si votre banque de données était formatée avec VMFS-2, vous pouvez lire les fichiers stockés sur VMFS-2, mais vous ne pouvez pas écrire dedans. Pour avoir un accès complet aux fichiers, mettez à niveau de VMFS-2 à VMFS-3.

Quand vous mettez à niveau VMFS-2 à VMFS-3, le mécanisme de verrouillage de fichier ESX assure qu'aucun processus local ou distant n'accède au volume de VMFS en conversion. Votre hôte préserve tous les fichiers sur la banque de données.

Par précaution, avant d'utiliser l'option de mise à niveau, prenez les éléments suivants en compte :

- Validez ou annulez les modifications aux disques virtuels dans le volume VMFS-2 que vous envisagez de mettre à niveau.
- Sauvegardez le volume VMFS-2.
- Assurez-vous que les machines virtuelles activées n'utilisent pas ce volume VMFS-2.
- Assurez-vous qu'aucun autre hôte ESX n'accède au volume VMFS-2.

La conversion VMFS-2 à VMFS-3 est un processus à sens unique. Après la conversion de la banque de données VMFS en VMFS-3, vous ne pouvez pas retourner à la version VMFS-2.

Pour mettre à niveau un système de fichiers VMFS-2, sa taille de bloc de fichier ne doit pas dépasser 8 Mo.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez un hôte dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Stockage]** .

3 Sélectionnez la banque de données qui utilise le format VMFS-2.

4 Cliquez sur **[Mise à niveau à VMFS-3]** .

5 Effectuez une nouvelle analyse de tous les hôtes voyant la banque de données.

Administration des banques de données VMFS dupliquées

Lorsqu'un LUN contient une copie de banque de données VMFS, vous pouvez monter la banque de données avec sa signature existante, ou lui assigner une nouvelle signature.

Chaque banque de données VMFS créée dans un LUN a un UUID unique qui est stocké dans le super-bloc de système de fichiers. Lorsque le LUN est répliqué ou capturé, la copie résultante identique, octet par octet, au LUN original. En conséquence, si le LUN initial contient une banque de données VMFS avec UUID X, la copie de LUN semble contenir une banque de données identique VMFS ou une copie de la banque de données VMFS, avec exactement le même UUID X..

ESX est capable de déterminer si un LUN contient une copie de banque de données VMFS, et peut monter la copie soit avec son UUID d'origine, ou changer l'UUID par re-signature de la banque de données.

Montage des banques de données VMFS avec des signatures existantes

Vous n'aurez peut-être pas besoin de procéder à la resignature d'une copie VMFS de banque de données. Vous pouvez monter une copie de banque de données sans modifier sa signature.

Par exemple, vous pouvez maintenir des copies synchronisées des machines virtuelles sur un site secondaire, dans le contexte d'un plan de récupération après sinistre. En cas de sinistre sur le site primaire, vous pouvez monter la copie de banque de données et démarrer les machines virtuelles sur le site secondaire.

IMPORTANT Vous ne pouvez monter une copie banque de données VMFS que si elle ne se heurte pas à une banque de données VMFS déjà montée avec la même UUID. Pour monter la copie, la banque de données VMFS d'origine doit être hors-ligne.

Lorsque vous montez la banque de données VMFS, ESX autorise un accès à la fois en écriture et en lecture à la banque de données résidant sur la copie de LUN. La copie de LUN doit être autorisée en écriture. Les banque de données montées sont persistantes, et restent valides après redémarrage du système.

Du fait qu' ESX ne propose pas une resignature de la banque de données montée, il vous faudra la démonter avant resignature.

Montage d'une banque de données VMFS avec une signature existante

Si vous n'avez pas à re-signer la copie d'un banque de données VMFS, vous pouvez le monter sans chager sa signature.

Prérequis

Avant de monter une banque de données, effectuez une réanalyse de stockage de votre hôte pour qu'il mette à niveau son affichage des LUN qui lui sont présentés.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez le serveur dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Stockage]** dans le panneau Matériel.

3 Cliquez sur **[Ajouter stockage]** .

4 Sélectionnez le type de stockage **[Disque/LUN]** et cliquez sur **[Suivant]** .

5 De la liste des LUN, sélectionnez le LUN qui a un nom de banque de données affiché dans la colonne Étiquette VMFS et cliquez sur **[Suivant]** .

   Le nom présent dans la colonne Étiquette VMFS indique que le LUN contient une copie d'une banque de données VMFS existante.

6 Dans Options de montage, sélectionnez **[Garder signature existante]** .

7 Sur la page Prêt à terminer, passez en revue les informations de configuration de banque de données et cliquez sur **[Terminer]** .

Suivant

Si vous voulez plus tard re-signer la banque de données montée, vous devrez d'abord le démonter.

Re-signature de copies VMFS

Utilisez la re-signature de banque de données pour conserver les données stockées dans la copie de la banque de données VMFS. Lors d'une re-signature de copie VMFS, ESX assigne une nouvelle UUID et une nouvelle étiquette à la copie, et la monte en tant que banque de données distincte de l'original.

Le format par défaut de la nouvelle étiquette assignée à la banque de données et `snap-`*`snapID`*`-`*`oldLabel`*, où *snapID* est un nombre entier et *oldLabel* est l'étiquette de la banque de données d'origine.

Lorsque vous effectuez une re-signature de banque de données, prenez en compte les points suivants :

- La re-signature d'une banque de données est irréversible.
- La copie de LUN qui contient la banque de données VMFS pour la re-signature ne sera plus traitée comme copie de LUN.
- Une banque de données éparpillée ne peut être resignaturée que si toutes ses parties sont en ligne.
- Le processus de re-signature est tolérant aux pannes et aux incidents. Si le processus est interrompu, vous pourrez le reprendre plus tard.
- Vous pouvez monter la nouvelle banque de données VMFS sans risque de collision de son UUID avec l'UUID de toute autre banque de données, comme un parent ou enfant dans une hiérarchie de snapshots LUN.

Re-signer la copie d'une banque de données VMFS

Utilisez la re-signature de banque de données si vous voulez conserver les données stockées dans la copie de datastore VMFS.

Prérequis

Pour re-signer la copie d'une banque de données montée, vous devez d'abord le démonter.

Avant de re-signer une banque de données, VMFS, effectuez une réanalyse de stockage de votre hôte pour qu'il mette à niveau son affichage des LUN qui lui sont présentés et découvre les copies de LUN.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez le serveur dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Stockage]** dans le panneau Matériel.

3 Cliquez sur **[Ajouter stockage]** .

4 Sélectionnez le type de stockage **[Disque/LUN]** et cliquez sur **[Suivant]** .

5 De la liste des LUN, sélectionnez le LUN qui a un nom de banque de données affiché dans la colonne Étiquette VMFS et cliquez sur **[Suivant]** .

Le nom présent dans la colonne Étiquette VMFS indique que le LUN contient une copie d'une banque de données VMFS existant.

6 Dans Options de montage, sélectionnez **[Affecter nouvelle signature]** et cliquez sur **[Suivant]** .

7 Sur la page Prêt à Terminer, passez en revue les informations de configuration de banque de données et cliquez sur **[Terminer]** .

Suivant

Après avoir re-signé, vous devrez faire ce qui suit :

- Si la banque de données resignée contient des machines virtuelles, mettez à niveau les références sur la banque de données VMFS initiale dans les fichiers de la machine virtuelle, y compris les fichiers.`vmx`,`.vmdk`,`.vmsd`, et.`vmsn`.
- Pour mettre sous tension des machines virtuelles, enregistrez-les avec vCenter Server.

Utilisation des chemins multiples avec ESX

Pour conserver une connexion constante entre un hôte ESX et son stockage, ESX prend en charge les chemins multiples. Le chemins multiples est une technique permettant d'utiliser plusieurs chemins d'accès physique pour transférer des données entre l'hôte ESX et le périphérique de stockage externe.

En cas de défaillance d'un élément dans le réseau SAN, notamment un HBA, un commutateur ou un câble, ESX peut utiliser d'autres chemins physiques pour accéder au périphérique de stockage. Ce processus est connu comme basculement de chemin. En plus du basculement de chemin, le chemins multiples permet un équilibrage de charge, qui redistribue les charges E/S entre plusieurs chemins, réduisant ou supprimant ainsi les goulots d'étranglement.

Gestion des chemins multiples

Pour la gestion multivoie de stockage, ESX utilise une couche VMkernel spéciale nommée Architecture de stockage enfichable (PSA). Le PSA est une structure modulaire ouverte qui coordonne les opérations simultanées de plusieurs plug-ins multichemin (MPP).

Le plug-in multichemin VMkernel que ESX fournit par défaut est le VMware Native Multipathing Plug-In (NMP). Le NMP est un module extensible qui gère les sous-plugins. Il existe deux types de sous-plugins NMP : Storage Array Type Plug-Ins (SATP) et Path Selection Plug-Ins (PSP). SATP et PSP peuvent être intégrés et fournis par VMware ou par un tiers.

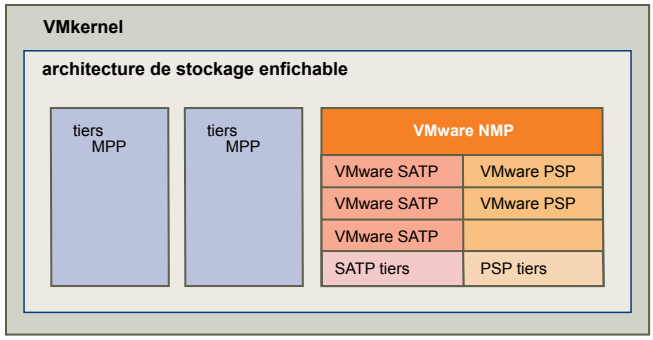
Si davantage de fonctionnalités de gestion multivoie sont nécessaires, un tiers peut également fournir un MPP à exécuter en complément ou en remplacement du NMP par défaut.

Lors de la coordination du VMware NMP et de tous les MPP tiers installés, la PSA effectue les tâches suivantes :

- Chargement et déchargement des plug-ins multichemin.
- Dissimulation des informations détaillées sur la machine virtuelle à un plug-in particulier.
- Routage des demandes d'E/S pour un périphérique logique spécifique vers le MPP qui gère ce périphérique.
- Traitement des files d'attente d'E/S vers les périphérique logiques.
- Mise en place du partage de la bande passante du périphérique logique entre les machines virtuelles.
- Traitement des files d'attente d'E/S vers les HBA de stockage physiques.
- Traitement de la détection et de la suppression des chemins physiques.
- Mise à disposition des statistiques d'E/S du périphérique logique et du chemin physique.

Comme Figure 9-1 l'illustre, plusieurs MPP tiers peuvent s'exécuter en parallèle avec le VMware NMP. Lorsqu'ils sont installés, les MPP tiers remplacent le comportement du NMP et prennent le contrôle total du basculement de chemin et des opérations d'équilibrage de charge pour les périphériques de stockage spécifiés.

Figure 9-1. Architecture de stockage enfichable



Les modules de gestion multivoie effectuent les opérations suivantes :

- Gestion des réclamations et des non réclamations de chemins physiques.
- Gestion de la création, de l'enregistrement et de l'annulation d'enregistrement des périphériques logiques.
- Association des chemins physiques avec les périphériques logiques.
- Prise en charge de la détection et de la correction des pannes de chemin.
- Traitement des demandes d'E/S vers les périphériques logiques :
  - Sélection d'un chemin physique optimal pour la demande.
  - Exécution, selon le périphérique de stockage, d'actions spécifiques nécessaires au traitement des défaillances de chemins et des nouvelles tentatives de commande d'E/S.
- Prise en charge des tâches de gestion, telles que l'interruption et la réinitialisation des périphériques logiques.

Module de gestion multivoie de VMware

Par défaut, ESX offrent un module multichemin extensible nommé Native Multipathing Plug-In (NMP).

De manière générale, le VMware NMP prend en charge toutes les baies de stockage répertoriées sur la liste de compatibilité matérielle (HCL) de stockage de VMware et fournit un algorithme de sélection de chemin par défaut reposant sur le type de baie. Le NMP associe une série de chemins physiques à un périphérique de stockage spécifique ou à une LUN. Les détails spécifiques du traitement du basculement de chemin pour une baie de stockage spécifique sont délégués au Storage Array Type Plugin (SATP). Les détails spécifiques de détermination du chemin physique utilisé pour émettre une demande d'E/S à un périphérique de stockage sont traités par un Path Selection Plugin (PSP). Les SATP et les PSP sont des sous-plugins dans le module NMP.

Suite à l'installation de ESX, le SATP approprié correspondant à la baie que vous utilisez sera installé automatiquement. Il n'est pas nécessaire d'obtenir ou de télécharger de SATP.

SATP de VMware

Les Storage Array Type Plug-Ins (SATP) s'exécutent avec VMware NMP et sont responsables des opérations spécifiques aux baies.

ESX offre un SATP pour chaque type de baie pris en charge par VMware. Il fournit également les SATP par défaut qui prennent en charge les baies de stockage non-spécifiques actives/actives et ALUA et le SATP local pour les périphériques directement reliés. Chaque SATP contient des caractéristiques spéciales d'une certaine classe de baies de stockage et effectue les opérations spécifiques à la baie nécessaires pour détecter l'état du chemin et pour activer un chemin inactif. Par conséquent, le module NMP peut fonctionner avec de nombreuses baies de stockage sans avoir à connaître les informations détaillées du périphérique de stockage.

Dès que le NMP détermine le SATP à utiliser pour un périphérique de stockage spécifique et qu'il associe le SATP aux chemins physiques de ce périphérique de stockage, le SATP met en œuvre les tâches suivantes :

- Surveillance du bon fonctionnement de chaque chemin physique.
- Rapports sur les modifications d'état de chaque chemin physique.
- Exécution d'actions spécifiques à la baie nécessaires pour le basculement du stockage. Par exemple, pour les périphériques actifs-passifs, il peut activer les chemins passifs.

PSP de VMware

Path Selection Plug-Ins (PSP) s'exécute avec VMware NMP et choisit un chemin physique pour les demandes d'E/S.

VMware NMP affecte un PSP par défaut pour chaque périphérique logique selon le SATP associé aux chemins physiques de ce périphérique. Vous pouvez remplacer le PSP par défaut.

Par défaut, le VMware NMP prend en charge les PSP suivants :

Dernière utilisation (VMW_PSP_MRU) Sélectionne le chemin que l'hôte ESX a le plus récemment utilisé pour accéder au périphérique. Si ce chemin est indisponible, l'hôte opte pour un autre chemin et continue d'utiliser le nouveau chemin tant qu'il est disponible. MRU est la règle de chemin par défaut pour les baies actives/passives.

Fixe (VMW_PSP_FIXED) Utilise le chemin favori s'il a été configuré. Sinon, il utilise le premier chemin opérationnel détecté au moment du démarrage du système. Si l'hôte n'est pas en mesure d'utiliser le chemin favori, il sélectionne de manière aléatoire un autre chemin disponible. L'hôte revient vers le chemin favori dès que celui-ci est disponible. Fixe est la règle de chemin par défaut pour les baies actives/actives.

AVERTISSEMENT Si elle est utilisée avec des baies actives/passives, la règle de chemin **[Fixe]** pourrait causer le vidage du chemin.

VMW_PSP_FIXED_AP Étend la fonctionnalité Fixe au baies actives/passives et de mode ALUA.

Round Robin (VMW_PSP_RR) Utilise un algorithme de sélection de chemins qui passe en revue tous les chemins actifs disponibles en activant l'équilibrage de charge sur les chemins.

Flux d'E/S de VMware NMP

Lorsqu'une machine virtuelle envoie une demande d'E/S à un périphérique de stockage géré par le NMP, le processus suivant a lieu :

1 Le NMP appelle le PSP assigné à ce périphérique de stockage.

2 Le PSP sélectionne le chemin physique approprié sur lequel il peut envoyer l'E/S.

3 Le NMP envoie la requête d'E/S sur le chemin sélectionné par le PSP.

4 Si l'opération d'E/S réussie, le NMP signale qu'elle est terminée.

5 Si l'opération d'E/S échoue, le NMP appelle le SATP approprié.

6 Le SATP interprète les erreurs de commande d'E/S et, si nécessaire, active les chemins inactifs.

7 Le PSP est appelé et sélectionne un nouveau chemin sur lequel il peut envoyer l'E/S.

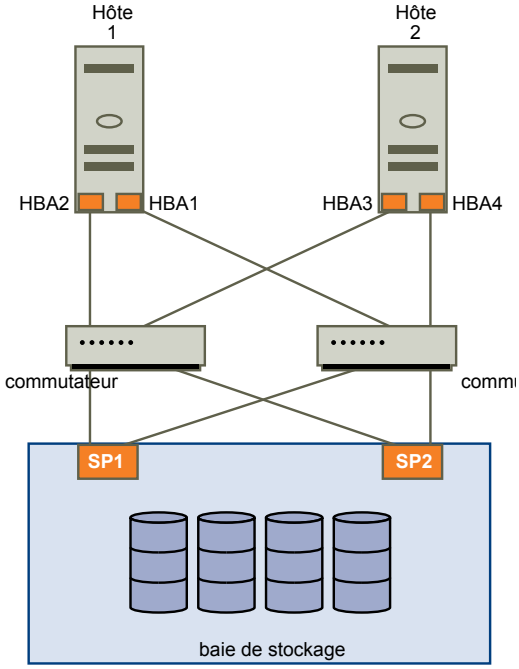
Chemins multiples avec stockage local et SAN Fibre Channel

Dans une topologie de stockage local à chemins multiples, vous pouvez utiliser un hôte ESX, qui a deux HBA. L'hôte ESX se connecte à un système de stockage local à deux ports via deux câbles. Cette configuration garantit une tolérance aux pannes si un des éléments de connexion entre l'hôte ESX et le système de stockage local est en panne.

Pour prendre en charge la commutation avec le SAN FC, l'hôte ESX a généralement plusieurs HBA disponibles à partir desquels la baie de stockage est atteignable à l'aide d'un ou plusieurs commutateurs. La configuration peut également inclure un HBA et deux processeurs de stockage afin que le HBA utilise un chemin différent pour atteindre la baie de disques.

Dans Figure 9-2, plusieurs chemins peuvent connecter chaque serveur au périphérique de stockage. Par exemple, si le HBA1 ou la liaison entre le HBA1 et le commutateur échoue, le HBA2 prend la relève et fournit la connexion entre le serveur et le commutateur. Le processus de reprise par un HBA pour un autre est appelé basculement HBA.

Figure 9-2. Chemins multiples Fibre Channel



De même, si le SP1 ou la liaison entre le SP1 et le commutateur s'interrompt, le SP2 prend la relève et fournit la connexion entre le commutateur et le périphérique de stockage. Ce processus est appelé basculement SP. ESX prend en charge le basculement HBA et SP pour sa capacité de chemins multiples.

Chemins multiples avec SAN iSCSI

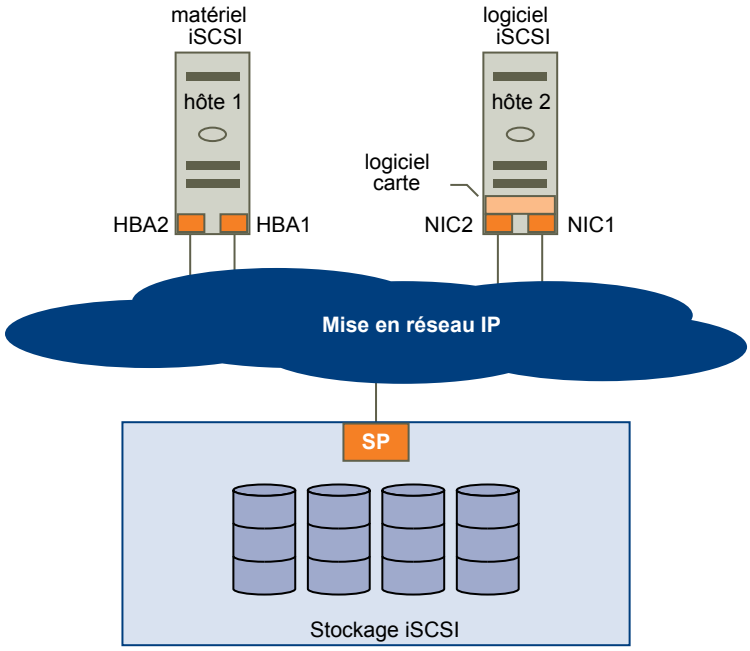
Avec le stockage iSCSI, vous pouvez tirer avantage de la prise en charge des chemins multiples que le réseau IP propose. Par ailleurs, ESX prend en charge les chemins multiples basés sur l'hôte pour tous les types d'initiateurs iSCSI.

ESX peut utiliser la prise en charge des chemins multiples intégrée au réseau IP, qui permet au réseau d'effectuer le routage. Grâce à la découverte dynamique, les initiateurs iSCSI obtiennent une liste des adresses cibles que les initiateurs peuvent utiliser comme chemins multiples vers les LUN iSCSI pour des objectifs de basculement.

ESX pend également en charge les chemins multiples basés sur l'hôte.

Figure 9-3 montre les configurations à chemins multiples possibles avec différents types d'initiateurs iSCSI.

Figure 9-3. Chemins multiples basés sur l'hôte



Chemins multiples avec iSCSI matériel

Avec le iSCSI matériel, l'hôte a généralement plusieurs adaptateurs iSCSI matériels disponibles à partir desquels le système de stockage peut être atteint à l'aide d'un ou plusieurs commutateurs. La configuration peut également inclure un adaptateur et deux processeurs de stockage afin que l'adaptateur utilise un chemin différent pour atteindre le système de stockage.

Dans l'illustration Figure 9-3, Hôte1 a deux adaptateurs iSCSI, HBA1 et HBA2, qui fournissent deux chemins physiques au système de stockage. Les plug-ins de chemins multiples sur votre hôte, qu'il s'agisse d'un NMP VMkernel ou de MPP tiers, ont accès aux chemins par défaut et peuvent surveiller la santé de chaque chemin physique. Si, par exemple, le HBA1 ou la liaison entre le HBA1 et le réseau échoue, les plug-ins de chemins multiples peuvent basculer le chemin sur le HBA2.

Chemins multiples avec iSCSI logiciel

Avec le iSCSI logiciel, comme indiqué sur Hôte 2 de Figure 9-3, vous pouvez utiliser plusieurs cartes d'interface réseau qui fournissent des fonctions de basculement et d'équilibrage de charge pour les connexions iSCSI entre votre hôte et les systèmes de stockage.

Pour cette configuration, comme les plug-ins de chemins multiples n'ont pas accès directement aux cartes d'interface réseau physiques sur votre hôte, vous devez connecter chaque carte d'interface réseau physique à un port VMkernel séparé. Vous associez ensuite tous les ports VMkernel à l'initiateur iSCSI logiciel à l'aide d'une technique de liaison de port. En conséquence, chaque port VMkernel connecté à un adapteur d'interface réseau séparée devient un chemin différent que la pile de stockage iSCSI et ses plug-ins de chemins multiples prenant en charge le stockage peuvent utiliser.

Pour plus d'informations sur la manière de configurer les chemins multiples pour l'iSCSI logiciel, voir « Configuration du réseau pour l'iSCSI logiciel et l'iSCSI matériel dépendant », page 75.

Analyse et réclamation des chemins

Lorsque vous démarrez votre hôte ESX ou réanalysez votre adaptateur de stockage, l'hôte découvre tous les chemins physiques aux périphériques de stockage disponibles sur l'hôte. En se basant sur un ensemble de règles de réclamation définies dans le fichier `/etc/vmware/esx.conf`, l'hôte détermine quel plug-in multichemin (MPP) doit réclamer les chemins à un périphérique particulier et devenir responsable de la gestion de cette prise en charge multichemin pour ce périphérique.

Par défaut, l'hôte effectue une évaluation périodique des chemins toutes les 5 minutes, faisant réclamer par le PPP approprié tous les chemins non réclamés.

Les règles de réclamation sont numérotées. Pour chaque chemin physique, l'hôte parcourt les règles de réclamation en commençant par le plus petit nombre. Les attributs du chemin physique sont comparés à la spécification de chemin dans la règle de réclamation. S'il trouve une correspondance, l'hôte assigne le MPP spécifié dans la règle de réclamation pour l'administration du chemin physique. Ce processus continue jusqu'à ce que tous les chemins physiques soient réclamés par les MPP correspondants, soit des plug-ins multichemin tiers, soit le plug-in multichemin natif (NMP).

Pour en savoir plus sur les plug-ins multichemin, reportez-vous à « Gestion des chemins multiples », page 128.

Pour les chemins administrés par le module NMP, un second ensemble de règles s'applique. Ces règles déterminent quel Storage Array Type Plug-In (SATP) doit être utilisé pour gérer les chemins pour un type spécifique de baie et quel Path Selection Plug-In (PSP) doit être utilisé pour chaque périphérique de stockage. Par exemple, pour un périphérique de stockage qui appartient à la famille de stockage EMC ClARiiON CX et n'est pas configuré comme matériel ALUA, le SATP par défaut est VMW_SATP_CX et le PSP par défaut est le plus récemment utilisé (Most Recently Used).

Utilisez le vSphere Client pour affciher le SATP et le PSP que l'hôte utilise pour un périphérique de stockage spécifique et le statut de tous les chemins disponibles pour ce périphérique de stockage. Au besoin, vous pouvez modifier le PSP VMware par défaut grâce au vSphere Client. Pour modifier le SATP par défaut, vous devez éditer les règles de réclamation dans vSphere CLI.

Pour plus d'informations sur les commandes disponibles pour gérer PSA, consultez le *Guide d'installation et de script de l'interface de ligne de commande de vSphere* et la *Référence de l'interface de ligne de commande vSphere*.

Affichage des informations sur les chemins

Utilisez le vSphere Client pour afficher le SATP et le PSP que l'hôte ESX utilise pour un support de stockage spécifique et le statut de tous les chemins disponibles pour ce périphérique de stockage. Vous pouvez accéder aux informations sur les chemins à la fois dans les fenêtres banque de données et Périphériques. Pour les banque de données, vous consultez les chemins connectés au périphérique hébergeant la banque de données.

Les informations du chemin comprennent le SATP assigné pour administrer le périphérique, la politique de sélection de chemins (PSP), et une liste de chemins avec leurs caractéristiques physiques, comme l'adaptateur et la cible utilisés, et le statut de chaque chemin. Les informations de statut du chemin suivantes peuvent s'afficher :

Active — Les chemins disponibles pour E/S avec un LUN. Un ou plusieurs chemins actifs en cours d'utilisation pour le transfert de données sont marqués comme Actifs (E/S).

Remarque Pour les hôtes faisant tourner ESX 3.5 ou plus anciens, le terme "Actif" désigne le chemin unique que l'hôte utilise pour E/S avec un LUN.

Veille — Le chemin est opérationnel et peut être utilisé pour E/S si les chamins actifs tombent en panne.

Désactivé Le chemin est désactivé et aucune donnée ne peut être transférée.

Mort Le logiciel ne peut joindre le disque par ce chemin.

Si vous utilisez la politique de chemin **[Fixe]** , vous pouvez voir quel est le chemin préféré. Le chemin préféré est marqué par une astérisque (*) dans la colonne Préféré.

Affichage des chemins d'accès aux banque de données

Utilisez vSphere Client pour examiner les chemins qui connectent les banque de données aux périphériques de stockage qui y sont déployés.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez un serveur dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Stockage]** dans le panneau Matériel.

3 Cliquez sur **[banque de données]** dans Vue.

4 Dans la liste des banque de données configurées, sélectionnez le datastore dont vous voulez afficher ou configurer les chemins.

Le volet Détails indique le nombre total de chemins pouvant accéder au périphérique et si l'un d'eux est cassé ou désactivé.

5 Cliquez sur **[Propriétés]** > **[Gérer les chemins]** pour ouvrir la boîte de dialogue Gérer les chemins.

Vous pouvez utiliser la boîte de dialogue Gérer les chemins pour activer ou mettre hors tension vos chemins, définir des règles de chemins multiples et spécifier le chemin préféré.

Affichage des chemins d'accès aux périphériques de stockage

Utilisez vSphere Client pour afficher quel SATP et PSP est utilisé par l'hôte pour un périphérique de stockage spécifique, et l'état de tous les chemins disponibles pour ce périphérique de stockage.

Procédure

1 Ouvrez une session sur vSphere Client et sélectionnez un serveur dans le panneau d'inventaire.

2 Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Stockage]** dans le panneau Matériel.

3 Cliquez sur **[Périphériques]** dans Vue.

4 Cliquez sur **[Gérer les chemins]** pour ouvrir la boîte de dialogue Gérer les chemins.

Définition d'une règle de sélection de chemin

Pour chaque périphérique de stockage, l'hôte ESX définit la règle de sélection de chemin d'accès basée sur les règles de réclamation définies dans le fichier `/etc/vmware/esx.conf`.

Par défaut, VMware prend en charge les règles de sélection de chemin d'accès suivantes. Si un PSP tiers est installé sur votre hôte, sa règle figure aussi dans la liste.

Fixe (VMW_PSP_FIXED) L'hôte utilise toujours le chemin d'accès préféré au disque quand ce chemin d'accès est disponible. Si l'hôte ne peut pas accéder au disque par le chemin d'accès préféré, il essaye les autres chemins d'accès. La règle par défaut pour les périphériques de stockage actifs-actifs est Fixe.

AP fixe (VMW_PSP_FIXED_AP) Étend la fonctionnalité Fixe aux baies actives/passives et de mode ALUA.

Dernière utilisation (VMW_PSP_MRU)

L'hôte sélectionne le chemin d'accès qui a été utilisé récemment. Quand le chemin d'accès devient non disponible, l'hôte sélectionne un autre chemin d'accès. L'hôte ne retourne pas au chemin d'accès d'origine quand ce chemin d'accès devient de nouveau disponible. Il n'y a aucun paramètre de chemin d'accès préféré avec la règle MRU. MRU est la règle par défaut pour les périphériques de stockage actifs-passifs.

Round Robin (VMW_PSP_RR)

L'hôte utilise un algorithme de sélection automatique de chemin d'accès qui effectue une permutation circulaire sur tous les chemins d'accès actifs lors de la connexion à des baies actives/passives ou sur tous les chemins d'accès disponibles lors de la connexion à des baies actives/actives. Cette option met en œuvre l'équilibrage de charge sur tous les chemins d'accès physiques disponibles pour l'hôte.

L'équilibrage de charge est le processus de distribution des requêtes d'E/S sur les chemins d'accès. Le but est d'optimiser les performances en termes de débit (E/S par seconde, mégaoctets par seconde ou temps de réponse).

Tableau 9-1 résume les changements de comportement de l'hôte en fonction du type de baie et des règles de basculement.

Tableau 9-1. Effets de la règle de chemin d'accès

Règle/Carte	Active/Active	Active/Passive
Most Recently Used	L'intervention de l'administrateur est requise pour la restauration suite à une défaillance sur un chemin d'accès.	L'intervention de l'administrateur est requise pour la restauration suite à une défaillance sur un chemin d'accès.
Fixe	VMkernel reprend en utilisant le chemin d'accès préféré lorsque la connectivité est restaurée.	VMkernel tente de reprendre en utilisant le chemin d'accès préféré. Cela peut provoquer l'annulation ou la défaillance du chemin d'accès si un autre SP possède maintenant le LUN.
Round Robin	Pas de restauration.	Le chemin d'accès suivant dans la planification Round Robin est sélectionné.
AP fixe	Pour les baies ALUA, VMkernel choisit le chemin d'accès défini comme chemin d'accès préféré. Pour les baies A/A, A/P et ALUA, VMkernel reprend en utilisant le chemins d'accès préféré, mais uniquement si l'algorithme évitant l'annulation des chemins d'accès autorise la restauration.	

Modification de la règle de sélection de chemin d'accès

Généralement, vous ne devez pas changer les paramètres multivoie par défaut que votre hôte utilise pour un périphérique de stockage spécifique. Cependant, si vous voulez faire des modifications, vous pouvez utiliser la boîte de dialogue Gérer Chemins d'accès pour modifier une règle de sélection de chemin d'accès et spécifier le chemin par défaut comme règle Fixe.

Procédure

1 Ouvrez la boîte de dialogue Gérer les chemins depuis la vue banque de données ou Périphériques.

2 Sélectionnez une règle de sélection de chemin d'accès.

Par défaut, VMware prend en charge les règles de sélection de chemin d'accès suivantes. Si un PSP tiers est installé sur votre hôte, sa règle figure aussi dans la liste.

- **[Fixe (VMW_PSP_FIXED)]**
- **[AP fixe (VMW_PSP_FIXED_AP)]**
- **[Dernière utilisation (VMW_PSP_MRU)]**
- **[Round Robin (VMW_PSP_RR)]**

3 Pour la règle fixe, spécifiez un chemin d'accès en cliquant avec le bouton droit de la souris sur le chemin à considérer comme votre chemin préféré, et sélectionnez **[Préféré]** .

4 Cliquez sur **[OK]** pour sauvegarder vos paramètres et quitter la boîte de dialogue.

Désactiver des chemins

Vous pouvez mettre hors tension temporairement certains chemins d'accès, pour des raisons de maintenance notamment. Pour cela, vous pouvez utiliser vSphere Client.

Procédure

1 Ouvrez la boîte de dialogue Gérer les chemins depuis la vue banque de données ou Périphériques.

2 Dans le panneau Paths, cliquez avec le bouton droit sur le chemin d'accès à mettre hors tension, puis sélectionnez **[Désactiver]** .

3 Cliquez sur **[OK]** pour sauvegarder vos paramètres et quitter la boîte de dialogue.

Vous pouvez également désactiver un chemin à partir de la vue Chemins de l'adaptateur : dans la liste, cliquez sur le chemin à l'aide du bouton droit de la souris, puis sélectionnez **[Désactiver]** .

Accélération matérielle du stockage

La fonctionnalité d'accélération matérielle permet à votre hôte de décharger des opérations d'une machine virtuelle spécifique et de gestion du stockage vers du matériel de stockage compatible. Avec l'assistance matérielle du stockage, votre hôte effectue les opérations plus rapidement et consomme moins de CPU, de mémoire et de bande passante de stockage.

Pour mettre en œuvre la fonctionnalité d'accélération matérielle, l'Architecture de stockage enfichable (PSA) utilise une association spéciale de plug-ins d'intégration de baies appelés plu-ins VAAI et un filtre d'intégration de baies, appelé filtre VAAI. Le PSA associe automatiquement le filtre VAAI et des plug-ins VAAI spécifiques au fournisseur aux périphériques de stockage qui prennent en charge l'accélération matérielle.

Pour afficher et gérer le filtre VAAI et les plug-ins VAAI disponibles sur votre hôte, utilisez les commandes de vSphere CLI.

Pour obtenir la description des commandes, voir *Guide d'installation et script de l'interface de ligne de commande vSphere* et *Référence de l'interface de ligne de commande vSphere*.

Contraintes et avantages de l'accélération matérielle

La fonctionnalité d'accélération matérielle fonctionne uniquement si vous utilisez une association hôte/baie de stockage appropriée.

Utilisez les hôtes et les baies de stockage suivants :

- ESX version 4.1 ou ultérieure.
- Baies de stockage prenant en charge l'accélération matérielle basée sur le stockage. ESX version 4.1 ne prend pas en charge l'accélération matérielle avec des périphériques de stockage NAS.

Sur votre hôte, l'accélération matérielle est activée par défaut. Pour activer l'accélération matérielle du côté du stockage, consultez le fournisseur du stockage. Certaines baies de stockage nécessitent que vous activiez la prise en charge de l'accélération matérielle explicitement du côté de stockage.

Lorsque la fonctionnalité d'accélération matérielle est prise en charge, l'hôte peut obtenir une assistance matérielle et effectuer les opérations suivantes plus rapidement et plus efficacement :

- Migration des machines virtuelles avec vMotion
- Déploiement des machines virtuelles à partir de modèles
- Clonage des machines virtuelles ou des modèles
- Verrouillage en cluster VMFS et opérations de métadonnées pour les fichiers des machines virtuelles
- Écriture vers des disques virtuels à allocation dynamique et lourds
- Création de machines virtuelles tolérant les pannes

État de la prise en charge de l'accélération matérielle

Pour chaque périphérique de stockage et banque de données, vSphere Client affiche l'état de prise en charge de l'accélération matérielle dans la colonne Accélération matérielle de la vue Périphériques et de la vue banque de données.

Les valeurs d'état sont Inconnu, Pris en charge et Non pris en charge. La valeur initiale est Inconnu. L'état passe à Pris en charge après que l'hôte a effectué avec succès l'opération de déchargement. Si l'opération de déchargement échoue, l'état passse à Non pris en charge.

Lorsque les périphériques de stockage ne prennent pas en charge ou fournissent uniquement une prise en charge partielle des opérations de l'hôte, votre hôte revient à ses méthodes natives d'exécution des opérations non pris en charge.

Désactivation de l'accélération matérielle

Si vos périphériques de stockage ne prennent pas en charge la fonctionnalité d'accélération matérielle, vous pouvez la désactiver à l'aide des paramètres avancés de vSphere Client.

Comme pour tous les paramètres avancés, avant de mettre hors tension l'accélération matérielle, contactez l'équipe de support de VMware.

Procédure

1 Dans le panneau d'inventaire de vSphere Client, sélectionnez l'hôte.

2 Dans l'onglet **[Configuration]** , cliquez sur **[Paramètres avancés]** sous **[Logiciel]** .

3 Cliquez sur VMFS3 et mettez à zéro la valeur du champ **[VMFS3.HardwareAcceleratedLocking]** .

4 Cliquez sur **[DataMover]** et mettez à zéro la valeur de chacun des champs suivants :

- **[DataMover.HardwareAcceleratedMove]**
- **[DataMover.HardwareAcceleratedInit]**

5 Cliquez sur **[OK]** pour enregistrer vos modifications.

Allocation dynamique

Lorsque vous créez une machine virtuelle, une certaine quantité d'espace de stockage sur une banque de données est provisionnée ou allouée aux fichiers du disque virtuel.

Par défaut, ESX offre une méthode d'allocation de stockage classique au cours de la création dans laquelle vous estimez la quantité de stockage dont la machine virtuelle aura besoin pour tout son cycle de vie, vous allouez une quantité fixe d'espace de stockage à son disque virtuel et associez tout l'espace alloué au disque virtuel. Un disque virtuel qui occupe immédiatement tout l'espace alloué est appelé un disque lourd. La création de disque virtuels au format lourd peut aboutir à une sous-utilisation de la capacité de la banque de données, car de grandes quantités d'espace de stockage, pré-alloué à différentes machines virtuelles, peuvent rester non utilisées.

Pour aider à éviter la sur-allocation de l'espace de stockage et à économiser du stockage, ESX prend en charge l'allocation dynamique qui vous permet, au début, d'utiliser uniquement la capacité de stockage dont vous avez besoin, puis d'ajouter la quantité nécessaire d'espace de stockage ultérieurement. Grâce à la fonction d'allocation dynamique de ESX, vous pouvez créer des disques virtuel au format léger. Pour un disque virtuel léger, ESX alloue tout l'espace requis pour les activités actuelles et futures du disque, mais ne valide que l'espace de stockage nécessaire aux opérations initiales.

À propos des formats de disque virtuel

Quand vous exécutez certaines opérations de gestion de machine virtuelle, par exemple la création d'un disque virtuel, le clonage d'une machine virtuelle dans un modèle ou le transfert d'une machine virtuelle, vous pouvez désigner un format pour le fichier de disque virtuel.

Les formats de disque suivants sont pris en charge. Vous ne pouvez pas indiquer le format de disque si le disque réside sur une banque de données NFS. Le serveur NFS détermine la règle d'allocation du disque.

Format à approvisionnement en allégé

Employez ce format pour économiser de l'espace de stockage. Pour le disque léger, vous fournissez autant d'espace de banque de données que le disque en exigerait d'après la valeur que vous saisissez comme taille de disque. Toutefois, le disque à approvisionnement en allégé commence par être petit et n'utilise dans un premier temps que l'espace de banque de données dont il a effectivement besoin pour ses opérations initiales.

REMARQUE Si un disque virtuel admet les solutions de cluster telles que la tolérance aux pannes, vous ne pouvez pas mettre le disque en allégé.

Si le disque à approvisionnement en allégé nécessite plus d'espace par la suite, il peut grandir jusqu'à sa capacité maximale et occuper l'intégralité de l'espace de banque de données qui lui a été affecté. En outre, vous pouvez convertir manuellement le disque léger en disque lourd.

Format lourd

Il s'agit du format de disque virtuel par défaut. Le disque virtuel au format lourd ne change pas de taille et occupe d'emblée l'intégralité de l'espace de banque de données qui lui est affecté. Il n'est pas possible de convertir le disque lourd en disque léger.

Création de disques virtuels alloués dynamiquement

Lorsque vous devez économiser l'espace de stockage, vous pouvez créer un disque virtuel au format alloué dynamiquement. Le disque virtuel alloué dynamiquement démarre avec une petite taille et grandit au fur et à mesure que de l'espace disque est nécessaire.

Cette procédure suppose que vous créiez une machine virtuelle personnalisée ou classique à l'aide de l'assistant Nouvelle machine virtuelle.

Prérequis

Vous pouvez créer des disques alloués dynamiquement uniquement sur les banque de données prenant en charge l'allocation dynamique. Si un disque réside sur une banque de données NFS, vous ne pouvez pas définir le format de disque, car le serveur NFS détermine la règle d'allocation pour le disque.

Procédure

- Dans la boîte de dialogue Créer un disque, sélectionnez **[Allouer et valider l'espace à la demande (provisionnement mince)]** .

Un disque virtuel au format alloué dynamiquement est créé. Si vous ne sélectionnez pas l'option Provisionnement mince, votre disque virtuel a le format lourd par défaut.

Suivant

Si vous avez créé un disque virtuel au format alloué dynamiquement, vous pouvez l'agrandir à sa taille totale ultérieurement.

Affichage des ressources de stockage des machines virtuelles

Vous pouvez consulter comment l'espace de stockage est alloué pour vos machines virtuelles.

Procédure

1. Sélectionnez la machine virtuelle dans l'inventaire.
2. Cliquez sur l'onglet **[Résumé]** .
3. Vérifiez les informations d'allocation d'espace dans la section Ressources.
   - Stockage provisionné : affiche l'espace de la banque de données garanti à la machine virtuelle. Tout l'espace ne peut pas être utilisé par la machine virtuelle si elle a des disques au format à allocation dynamique. D'autres machines virtuelles peuvent occuper l'espace non utilisé.
   - Stockage non partagé : affiche l'espace de banque de données occupé par la machine virtuelle et non partagé avec d'autres machines virtuelles.
   - Stockage utilisé : affiche l'espace de banque de données réellement occupé par les fichiers de la machine virtuelle, y compris les fichiers de configuration et journaux, les snapshots, les disques virtuels, etc. Lorsque la machine virtuelle est en fonctionnement, l'espace de stockage utilisé comprend également les fichiers d'échange.

Déterminer le format de disque d'une machine virtuelle

Vous pouvez déterminer si votre disque virtuel est au format léger ou lourd.

Procédure

1. Sélectionnez la machine virtuelle dans l'inventaire.
2. Cliquez sur **[Modifier les paramètres]** pour afficher la boîte de dialogue Propriétés de machine virtuelle.

3 Cliquez sur l'onglet **[Matériel]** et sélectionnez le disque dur approprié dans la liste de matériel.

La section Provisionnement disque sur le côté droit présente le type de votre disque virtuel, léger (Thin) ou lourd (Thick).

4 Cliquez sur **[OK]** .

Suivant

Si votre disque virtuel est au format léger, vous pouvez le gonfler à la taille normale.

Convertir un disque virtuel léger en disque virtuel épais

Si vous avez créé un disque virtuel au format léger, vous pouvez le convertir en lourd.

Procédure

1 Sélectionnez la machine virtuelle dans l'inventaire.

2 Cliquez sur l'onglet **[Résumé]** et, sous Ressources, double-cliquez sur la banque de données pour que la machine virtuelle ouvre la boîte de dialogue Navigateur de banque de données.

3 Cliquez sur le dossier de machine virtuelle pour trouver le fichier de disque virtuel que vous voulez convertir. Le fichier porte l'extension `.vmdk`.

4 Cliquez avec le bouton droit sur le fichier de disque virtuel et sélectionnez **[Gonfler]** .

Le disque virtuel au format lourd occupe l'espace entier de la banque de données qui lui était attribué à l'origine.

Traitement du sur-abonnement de banque de données

Comme l'espace alloué pour les disques légers peut être supérieur à l'espace validé, un sur-abonnement de la banque de données peut survenir, ce qui fait que l'espace total alloué pour les disques de la machine virtuelle sur la banque de données est supérieur à la capacité réelle.

Le sur-abonnement peut être possible, car toutes les machines virtuelles à disques légers n'ont généralement pas besoin de tout l'espace de banque de données alloué en même temps. Cependant, si vous souhaitez éviter le sur-abonnement à la banque de données, vous pouvez configurer une alarme qui vous avertit lorsque l'espace alloué atteint un certain seuil.

Pour plus d'informations sur la configuration d'alarme, voir le *Guide d'administration du centre de données VMware vSphere*.

Si vos machines virtuelles nécessitent plus d'espace, l'espace de la banque de données est alloué sur la base du premier arrivé, premier servi. Lorsque la banque de données est à court d'espace, vous pouvez ajouter plus de stockage physique et augmenter la banque de données.

Reportez-vous à « Augmentation des banques de données VMFS », page 124.

Désactiver les filtres de stockage vCenter Server

Lorsque vous effectuez des opérations de gestion de banque de données VMFS, vCenter Server utilise des filtres de stockage par défaut. Les filtres vous aident à éviter une corruption du stockage en extrayant uniquement les périphériques de stockage, ou LUN, pouvant être utilisés pour une opération particulière. Les LUN non conformes ne sont pas affichés pour la sélection. Vous pouvez mettre hors tension les filtres pour afficher tous les LUN.

Avant d'apporter des modifications aux filtres des LUN, contactez l'équipe de support de VMware. Vous pouvez mettre hors tension les filtres uniquement si vous avez d'autres moyens d'empêcher une corruption des LUN.

Procédure

1 Dans vSphere Client, sélectionnez **[Administration] > [Paramètres vCenter Server]** .

2 Dans la liste des paramètres, sélectionnez **[Paramètres avancés]** .

3 Dans la zone de texte **[Touche]** , entrez une clé.

Touche	Nom du filtre
config.vpxd.filter.vmfsFilter	Filtre VMFS
config.vpxd.filter.rdmFilter	Filtre RDM
config.vpxd.filter.SameHostAndTransportsFilter	Filtre d'hôte et de transports identique
config.vpxd.filter.hostRescanFilter	Filtre de réanalyse d'hôte **REMARQUE** Si vous désactivez le filtre de réanalyse de l'hôte, vos hôtes continuent d'exécuter une réanalyse à chaque fois que vous présentez un nouveau LUN à un hôte ou un cluster.

4 Dans la zone de texte **[Valeur]** , tapez **Faux** pour la clé spécifiée.

5 Cliquez sur **[Ajouter]** .

6 Cliquez sur **[OK]** .

Vous n'avez pas besoin de redémarrer le système vCenter Server.

Filtrage du stockage de vCenter Server

vCenter Server fournit des filtres de stockage pour vous aider à éviter la corruption des périphériques de stockage ou des dégrations de performances pouvant être provoquées par une utilisation non prise en charge des LUN. Ces filtres sont disponibles par défaut.

Tableau 9-2. Filtres de stockage

Nom du filtre	Description	Touche
Filtre VMFS	Élimine les périphériques de stockage, ou LUN, qui sont déjà utilisés par une banque de données VMFS ou un hôte géré par vCenter Server. Les LUN ne s'affichent pas comme des candidats au formatage avec une autre banque de données VMFS ou pour une utilisation en tant que RDM.	config.vpxd.filter.vmfsFilter
Filtre RDM	Élimine les LUN déjà référencés par un RDM sur un hôte géré par vCenter Server. Les LUN ne s'affichent pas comme des candidats au formatage avec VMFS ou pour une utilisation par un RDM différent. Si vos machines virtuelles doivent accéder au même LUN, celles-ci doivent partager le même fichier de mappage RDM. Pour plus d'informations sur ce type de configuration, voir *Configuration d'un cluster de basculement et du service de cluster de Microsoft.*	config.vpxd.filter.rdmFilter

Tableau 9-2. Filtres de stockage (suite)

Nom du filtre	Description	Touche
Filtre d'hôte identique et de transports	Élimine les LUN inéligibles pour une utilisation comme extensions de banque de données VMFS en raison d'incompatibilié d'hôte ou de stockage. Vous empêche d'ajouter les LUN suivants comme extensions : ■ LUN non exposés à tous les hôtes qui partagent la banque de données VMFS d'origine. ■ LUN utilisant un type de stockage différent de celui utilisé par la banque de données d'origine. Par exemple, vous ne pouvez pas ajouter une extension Fibre Channel à une banque de données VMFS sur un périphérique de stockage local.	config.vpxd.filter.SameHostAndTransportsFilter
Filtre de réanalyse d'hôte	Réanalyse automatiquement et met à niveau les banque de données VMFS après que vous avez effectué des opérations de gestion de banque de données. Ce filtre aide à fournir une vue cohérente de toutes les banque de données VMFS sur tous les hôtes gérés par vCenter Server. **Remarque** Si vous présentez un nouveau LUN à un hôte ou un cluster, les hôtes exécutent automatiquement une réanalyse que le filtre de réanalyse d'hôte soit activé ou non.	config.vpxd.filter.hostRescanFilter

Mappage de périphérique brut 10

Le mappage de périphérique brut (RDM) fournit un mécanisme permettant à une machine virtuelle d'accéder directement à un LUN sur le sous-système de stockage physique (Fibre Channel ou iSCSI uniquement).

Les rubriques suivantes contiennent des informations sur les RDM et fournissent des instructions sur la manière de créer et de gérer des RDM.

Ce chapitre aborde les rubriques suivantes :

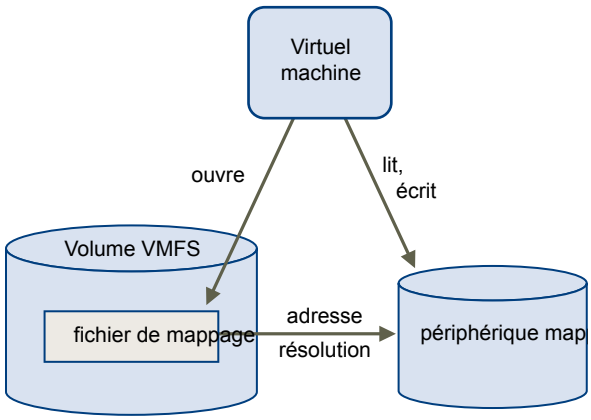
À propos du mappage de périphérique brut

Le RDM est un fichier de mappage dans un volume VMFS séparé qui agit comme un proxy pour un périphérique de stockage physique brut. Le RDM permet à une machine virtuelle d'accéder directement au périphérique de stockage et de l'utiliser. Le RDM contient des métadonnées pour la gestion et la redirection de l'accès au disque vers le périphérique physique.

Le fichier vous donne certains des avantages de l'accès direct au périphérique physique tout en conservant les avantages du disque virtuel dans VMFS. En conséquence, il associe la capacité de gestion de VMFS à l'accès au périphérique brut.

Les RDM peuvent être décrits comme le mappage d'un périphérique brut dans une banque de données, le mappage d'un LUN système ou le mappage d'un fichier du disque vers un volume de disque physique. Tous ces termes se rapportent au RDM.

Figure 10-1. Mappage de périphérique brut



Bien que VMware recommande d'utiliser les banque de données VMFS pour la plus grande partie du stockage sur disque virtuel, dans certains cas, vous pouvez utiliser des LUN bruts ou des disques logiques situés sur un SAN.

Par exemple, vous pouvez utiliser des LUN bruts avec des RDM dans les situations suivantes :

- Lorsque le snapshot du SAN ou d'autres applications en couche sont exécutés dans la machine virtuelle. Le RDM permet des systèmes de déchargement évolutifs à l'aide de fonctions inhérentes au SAN.
- Dans tout scénario de mise en clusters MSCS qui parcourt les hôtes physiques (clusters virtuel à virtuel ainsi que clusters physique à virtuel). Dans ce cas, les données du cluster et les disques quorum doivent configurés comme des RDM plutôt que comme des fichiers sur un VMFS partagé.

Considérez un RDM comme un lien symbolique d'un volume VMFS vers un LUN brut. Le mappage fait apparaître les LUN comme des fichiers dans un volume VMFS. LE RDM, et non le LUN brut, est référencé dans la configuration de la machine virtuelle. Le RDM contient une référence au LUN brut.

En utilisant le RDM, vous pouvez :

- Utiliser vMotion pour migrer des machines virtuelles à l'aide de LUN bruts.
- Ajouter des LUN bruts aux machines virtuelles à l'aide de vSphere Client.
- Utiliser les fonctions du système de fichiers telles que le verrouillage des fichiers distribués, les autorisations et les noms.

Deux modes de compatibilité sont disponibles pour les RDM :

- Le mode de compatibilité virtuelle permet à un RDM d'agir exactement comme un fichier de disque virtuel, y compris l'utilisation des snapshots.
- Le mode de compatibilité physique permet un accès direct au périphérique SCSI pour les applications ayant besoin d'un niveau de contrôle inférieur.

Avantages du mappage de périphérique brut

Un RDM fournit un certain nombre d'avantages, mais il ne doit pas être utilisé dans tous les cas. Généralement, les fichiers de disque virtuel sont préférables à la capacité de gestion du RDM. Cependant, si vous avez besoin de périphériques bruts, vous devez utiliser le RDM.

Le RDM offre plusieurs avantages.

Noms persistants conviviaux
Fournit un nom convivial pour un périphérique mappé. Lorsque vous utilisez un RDM, il est inutile de se rapporter au périphérique par son nom de périphérique. Vous l'appelez par le nom du fichier de mappage, par exemple :

```
/vmfs/volumes/monVolume/monRépertoireVM/myonDisqueBrut.vmdk
```

Résolution dynamique de nom
Stocke des informations uniques d'identification pour chaque périphérique mappé. VMFS associe chaque RDM à son périphérique SCSI actuel, quelles que soient les modifications dans la configuration physique du serveur, en raison des modifications matérielles de l'adaptateur, des modifications de chemin, de la relocalisation du périphérique, etc.

Verrouillage des fichiers distribués
Permet d'utiliser le verrouillage distribué VMFS pour les périphériques SCSI bruts. Le verrouillage distribué sur un RDM permet d'utiliser en toute sécurité un LUN brut partagé sans perdre de données lorsque deux machines virtuelles sur des serveurs différents essaient d'accéder au même LUN.

Autorisations de fichier
Permet les autorisations de fichier. Les autorisations de fichier de mappage sont appliquées au moment de l'ouverture du fichier pour protéger le volume mappé.

Opérations du système de fichiers

Permet d'utiliser les utilitaires du système de fichiers pour travailler avec un volume mappé à l'aide du fichier de mappage comme proxy. La plupart des opérations valides pour un fichier ordinaire peuvent être appliquées au fichier de mappage et sont redirigées pour fonctionner sur un périphérique mappé.

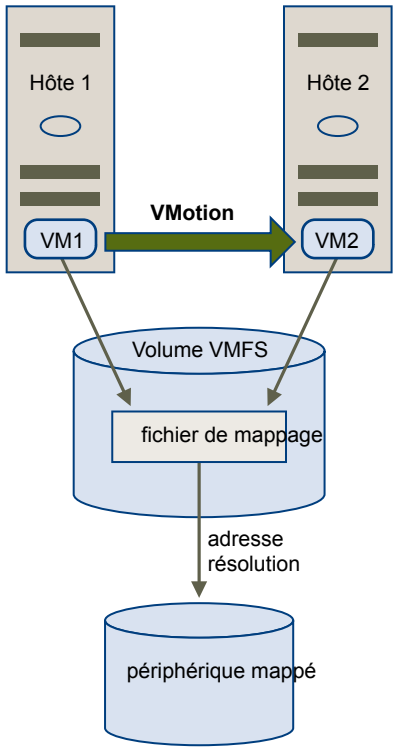
Snapshots

Permet d'utiliser les snapshots de machine virtuelle sur un volume mappé. Les snapshots ne sont pas disponibles lorsque le RDM est utilisé en mode de compatibilité physique.

vMotion

Permet de migrer une machine virtuelle avec vMotion. Le fichier de mappage agit comme un proxy pour permettre à vCenter Server de migrer la machine virtuelle à l'aide du même mécanisme que celui qui existe pour la migration des fichiers du disque.

Figure 10-2. vMotion pour une machine virtuelle utilisant le mappage de périphérique brut



Agents de gestion du SAN

Permet d'exécuter certains agents de gestion du SAN à l'intérieur d'une machine virtuelle. De même, tout logiciel ayant besoin d'accéder à un périphérique à l'aide de commandes SCSI spécifiques au matériel peut être exécuté dans une machine virtuelle. Ce type de logiciel est appelé logiciel basé sur cible SCSI. Lorsque vous utilisez les agents de gestion du SAN, sélectionnez un mode de compatibilité physique pour le RDM.

Virtualisation d'ID de port N (NPIV)

Permet d'utiliser la technologie NPIV qui autorise un port unique Fibre Channel HBA à s'enregistrer sur l'ensemble Fibre Channel à l'aide de plusieurs noms de port mondiaux (WWPN). Ainsi, le port HBA a la forme de ports virtuels multiples, chacun ayant son propre ID et un nom de port virtuel. Les machines virtuelles peuvent ensuite appeler chacun de ces ports virtuels et les utiliser pour tout le trafic RDM.

Remarque Vous ne pouvez utiliser le NPIV qu'avec les machines virtuelles dotées de disques RDM.

VMware travaille avec les fournisseurs de logiciel de gestion de stockage pour garantir que leur logiciel fonctionne correctement dans des environnements incluant ESX. Certaines applications de ce type sont :

- Logiciel de gestion du SAN
- Logiciel de gestion des ressources de stockage (SRM)
- Logiciel de snapshot
- Logiciel de réplication

De tels logiciels utilisent un mode de compatibilité physique pour les RDM afin que le logiciel puisse accéder aux périphériques directement.

Divers produits de gestion s'exécutent mieux de manière centralisée (non pas sur la machine ESX), tandis que d'autres s'exécutent bien sur la console du service ou sur les machines virtuelles. VMware ne certifie pas ces applications, ni ne fournit de matrice de compatibilité. Pour savoir si une application de gestion du SAN est prise en charge dans un environnement ESX, contactez le fournisseur du logiciel de gestion du SAN.

Limitations du mappage de périphérique brut

Certaines limitations existent lorsque vous utilisez les RDM.

- Non disponible pour les périphériques de traitement par blocs sur certains périphériques RAID : le RDM utilise un numéro de série pour identifier le périphérique mappé. Comme les périphériques de traitement par blocs et certains périphériques RAID à connexion directe n'exportent pas de numéros de série, ils ne peuvent pas être utilisés avec les RDM.
- Disponible avec les volumes VMFS-2 et VMFS-3 uniquement : le RDM nécessite le format VMFS-2 ou VMFS-3. Dans ESX, le système de fichiers VMFS-2 est en lecture seule. Mettez-le à niveau à VMFS-3 pour utiliser les fichiers que VMFS-2 stocke.
- Aucun snapshot dans le mode de compatibilité physique : si vous utilisez un RDM en mode de compatibilité physique, vous ne pouvez pas utiliser un snapshot avec le disque. Le mode de compatibilité physique permet à la machine virtuelle de gérer son propre snapshot ou de mettre en miroir des opérations.

  Les snapshots sont disponibles en mode virtuel.
- Aucun mappage de partition : le RDM nécessite que le périphérique mappé soit un LUN entier. Le mappage vers une partition n'est pas pris en charge.

Caractéristiques du mappage de périphérique brut

Un RDM est un fichier de mappage spécial dans un volume VMFS qui gère les métadonnées pour son périphérique mappé. Le fichier de mappage est présenté au logiciel de gestion comme un fichier de disque ordinaire, disponible pour les opérations fichier-système habituelles. Pour la machine virtuelle, la couche de visualisation du stockage présente le périphérique mappé comme un périphérique SCSI.

Le contenu clé des métadonnées du fichier de mappage comprend l'emplacement du périphérique mappé (résolution de nom), l'état de verrouillage du périphérique mappé, les autorisations, etc.

Modes de compatibilité physique et virtuel du RDM

Vous pouvez utiliser les RDM en mode de compatibilité virtuelle ou en mode de compatibilité physique. Le mode virtuel spécifie la virtualisation totale du périphérique mappé. Le mode physique spécifie une virtualisation SCSI minimale du périphérique mappé, permettant une plus grande flexibilité pour le logiciel de gestion du réseau SAN.

En mode virtuel, VMkernel envoie uniquement READ et WRITE au périphérique mappé. Le périphérique mappé apparaît pour le système d'exploitation invité exactement comme un fichier de disque virtuel dans un volume VMFS. Les caractéristiques réelles du matériel sont masquées. Si vous utilisez un disque brut en mode virtuel, vous pouvez vous rendre compte des avantages du VMFS tels que le verrouillage avancé du fichier pour la protection des données et les snapshots pour la rationalisation des processus de développement. Le mode virtuel est également plus compatible au sein du matériel de stockage que le mode physique et présente le même comportement qu'un fichier de disque virtuel.

En mode physique, VMkernel transmet toutes les commandes SCSI au périphérique, sans aucune exception : la commande REPORT LUN est virtualisée afin que VMkernel puisse isoler le LUN pour la machine virtuelle propriétaire. Sinon, toutes les caractéristiques physiques du matériel sous-jacent sont exposées. Le mode physique est utilisé pour exécuter les agents de gestion du SAN et d'autres logiciels basés sur cible SCSI dans la machine virtuelle. Le mode physique permet également une mise en cluster virtuel à physique pour une disponibilité rentable.

Résolution dynamique de nom

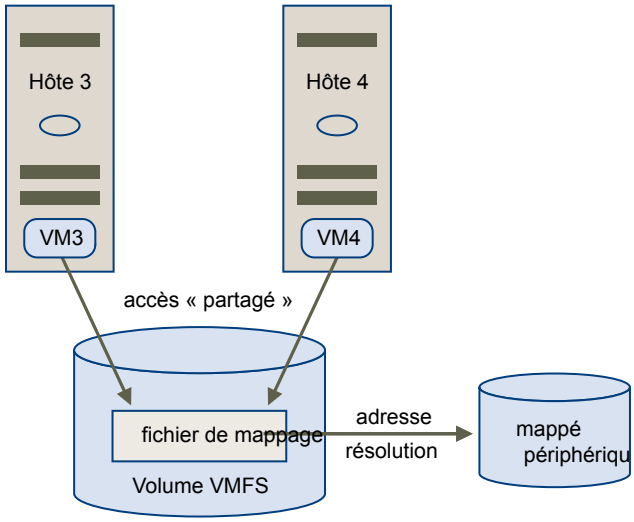
Le fichier RDM prend en charge la résolution dynamique de nom lorsqu'un chemin vers un périphérique brut change.

VMFS identifie de manière unique tous les périphériques de stockage mappés, et l'identification est stockée dans ses structures de données internes. Toute modification au chemin vers un périphérique brut, telle qu'une défaillance de commutateur Fibre Channel ou l'ajout d'un nouvel HBA, peut modifier le nom du périphérique. La résolution dynamique de nom résout ces modifications et associe automatiquement le périphérique d'origine à son nouveau nom.

Mappage de périphérique brut sur des clusters de machine virtuelle

Utilisez un RDM avec les clusters de machine virtuelle qui doivent accéder au même LUN brut pour les scénarios de reprise. La configuration est identique à celle d'un cluster de machine virtuelle accédant au même fichier de disque virtuel, mais un RDM remplace le fichier de disque virtuel.

Figure 10-3. Accès à partir des machines virtuelles en clusters



Comparaison des modes d'accès disponibles du périphérique SCSI

Les méthodes d'accès à un périphérique de stockage SCSI comprennent un fichier de disque virtuel sur une banque de données VMFS, un RDM de mode virtuel et un RDM de mode physique.

Pour vous aider à choisir parmi les modes d'accès disponibles pour les périphériques SCSI, Tableau 10-1 donne une brève comparaison des fonctions disponibles avec les différents modes.

Tableau 10-1. Fonctions disponibles dans les disques virtuels et les mappages de périphérique brut

Fonctions ESX	Fichier de disque virtuel	RDM mode virtuel	RDM mode physique
Commandes SCSI transmises	Non	Non	Oui REPORT LUN n'est pas transmis
Prise en charge vCenter Server	Oui	Oui	Oui
Snapshots	Oui	Oui	Non
Verrouillage distribué	Oui	Oui	Oui
Mettre en cluster	Cluster dans une boîte uniquement	Cluster dans une boîte et cluster entre boîtes	Cluster physique à virtuel
Logiciel basé sur cible SCSI	Non	Non	Oui

VMware recommande d'utiliser des fichiers de disque virtuel pour le type cluster dans une boîte de mise en cluster. Si vous envisagez de reconfigurer vos clusters cluster dans une boîte en clusters cluster-accross-the-box, utilisez les RDM de mode virtuel pour les clusters cluster dans une boîte.

Gestion des LUN mappés

Vous pouvez utiliser vSphere Client pour mapper un LUN de réseau SAN sur une banque de données et gérer les chemins vers votre LUN mappé.

Les outils supplémentaires pour gérer les LUN mappés et leurs RDM comprennent l'utilitaire `vmkfstools` et d'autres commandes utilisées avec vSphere CLI. Vous pouvez utiliser l'utilitaire `vmkfstools` pour effectuer de nombreuses opérations identiques disponibles via vSphere Client.

Vous pouvez également utiliser les commandes communes du système de fichiers dans la console du service.

Création de machines virtuelles avec des RDM

Quand vous donnez à votre machine virtuelle un accès direct à un LUN de réseau SAN brut, vous créez un fichier de mappage (RDM) qui réside sur une banque de données VMFS et pointe vers le LUN. Bien que le fichier de mappage possède l'extension.`vmdk` comme un fichier de disque virtuel standard, le fichier RDM contient seulement les informations de mappage. Les données réelles de disque virtuel sont stockées directement sur le LUN.

Vous pouvez créer le RDM comme un disque initial pour une nouvelle machine virtuelle ou l'ajouter à une machine virtuelle existante. Lors de la création du RDM, vous spécifiez le LUN à mapper et la banque de données sur laquelle mettre le RDM.

Procédure

1 Suivez toutes les étapes requises pour créer une machine virtuelle personnalisée.

2 Dans la page Choisir disque, sélectionnez **[Mappage de périphériques bruts]** , puis cliquez sur **[Suivant]** .

3 Dans la liste des disques du SAN ou des LUN, sélectionnez un LUN auquel votre machine virtuelle accède directement.

4 Sélectionnez une banque de données pour le fichier de mappage RDM.

Vous pouvez placer le fichier RDM sur la banque de données où réside votre fichier de configuration de machine virtuelle ou en sélection une autre.

Remarque Pour utiliser vMotion pour les machines virtuelles avec NPIV activé, assurez-vous que les fichiers RDM des machines virtuelles sont situés dans la même banque de données. Vous ne pouvez pas effectuer Storage vMotion ou vMotion entre des banque de données lorsque NPIV est activé.

5 Sélectionnez un mode de compatibilité.

Option	Description
Physique	Permet au système d'exploitation invité d'accéder directement au matériel. La compatibilité physique est utile si vous utilisez des applications prenant en charge les SAN sur la machine virtuelle. Cependant, les machines virtuelles sous tension utilisant des RDM et configurées pour la compatibilité physique ne peuvent pas être migrées si la migration suppose de copier le disque. Ces machines virtuelles ne peuvent pas être clonées, ni clonées en modèle.
Virtuel	Permet au RDM de se comporter comme s'il était un disque virtuel, afin que vous puissiez utiliser des fonctions telles que la prise de snapshots, le clonage, etc.

6 Sélectionnez un nœud de périphérique virtuel.

7 Si vous sélectionnez le mode Indépendant, choisissez l'une des options suivantes.

Option	Description
Persistent (Persistant)	Les changements sont immédiatement et définitivement écrits sur le disque.
Non permanent	Les modifications apportées au disque sont ignorées à la mise hors tension ou au rétablissement du snapshot.

8 Cliquez sur **[Suivant]** .

9 Dans la page Prêt à terminer Nouvelle machine virtuelle, vérifiez vos sélections.

10 Cliquez sur **[Terminer]** pour terminer votre machine virtuelle.

Gestion des chemins pour un LUN brut mappé

Vous pouvez gérer les chemins pour les LUN bruts mappés.

Procédure

1 Connectez-vous en tant qu'administrateur ou en tant que propriétaire de la machine virtuelle à laquelle le disque mappé appartient.

2 Sélectionnez la machine virtuelle dans le panneau d'inventaire.

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

4 Dans l'onglet **[Matériel]** , sélectionnez **[Disque dur]** , puis cliquez sur **[Gérer les chemins]** .

5 Utilisez la boîte de dialogue Gérer les chemins pour activer ou mettre hors tension vos chemins, définir la règle de chemins multiples et indiquer le chemin préféré.

Pour plus d'informations sur la gestion des chemins, voir « Utilisation des chemins multiples avec ESX », page 128.

Sécurité

Sécurité pour systèmes ESX 11

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

Ce chapitre aborde les rubriques suivantes :

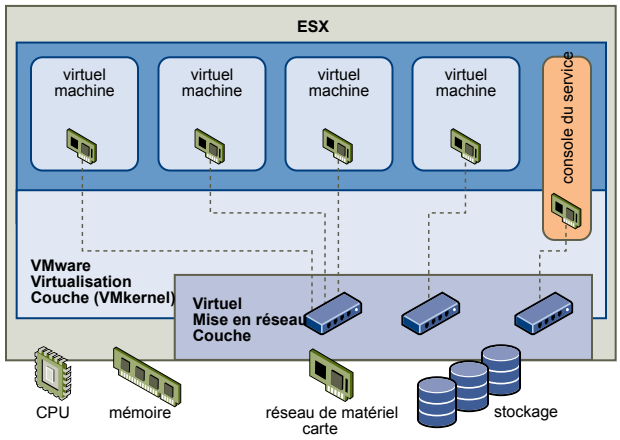
Architecture ESX et fonctions de sécurité

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

Sous l'angle de la sécurité, ESX contient quatre composants principaux : la couche de virtualisation, les machines virtuelles, la console de service et la couche réseau virtuelle.

Figure 11-1 présente ces composants.

Figure 11-1. Architecture ESX



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.

ESX offre une protection VMkernel supplémentaire pour les fonctions suivantes :

Durcissement de la mémoire — Le noyau ESX, 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 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 ESX d'identifier les fournisseurs des modules, pilotes ou applications concernés, et de vérifier s'ils sont dotés d'une certification VMware.

Sécurité et machines virtuelles

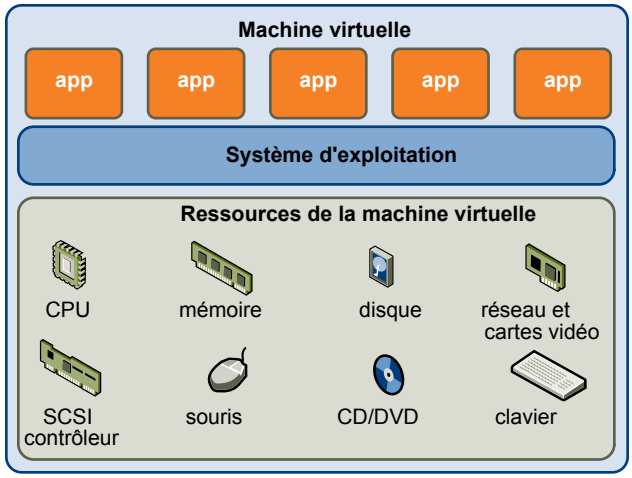
Les machines virtuelles sont les conteneurs dans lesquels sont exécutés les systèmes d'exploitation invités et les applications. Dès la conception, toutes les machines virtuelles VMware sont isolées les unes des autres. Cette isolation permet l'exécution en toute sécurité de plusieurs machines virtuelles 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 droits 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 autorisations explicitement accordées par l'administrateur système ESX. 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 ne peut pas détecter les autres unités virtuelles, comme illustré dans la Figure 11-2.

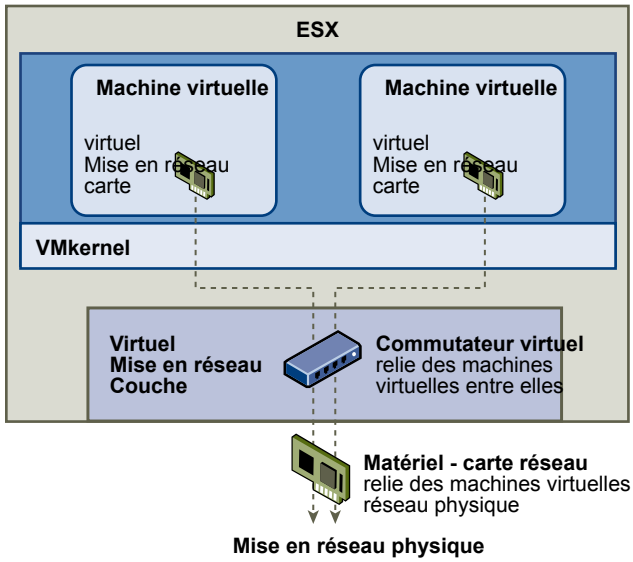
Figure 11-2. Isolation des machines virtuelles



VMkernel s'interpose entre les ressources physiques ; par ailleurs, tous les accès aux composants matériels s'effectuent via VMkermel ; 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 adapteur 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 ESX) via un adapteur réseau physique, comme l'illustre la Figure 11-3.

Figure 11-3. 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 adapteur 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 ESX, 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 ressouces 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, ESX 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 cartes réseau virtuelles et des commutateurs virtuels. ESX 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).

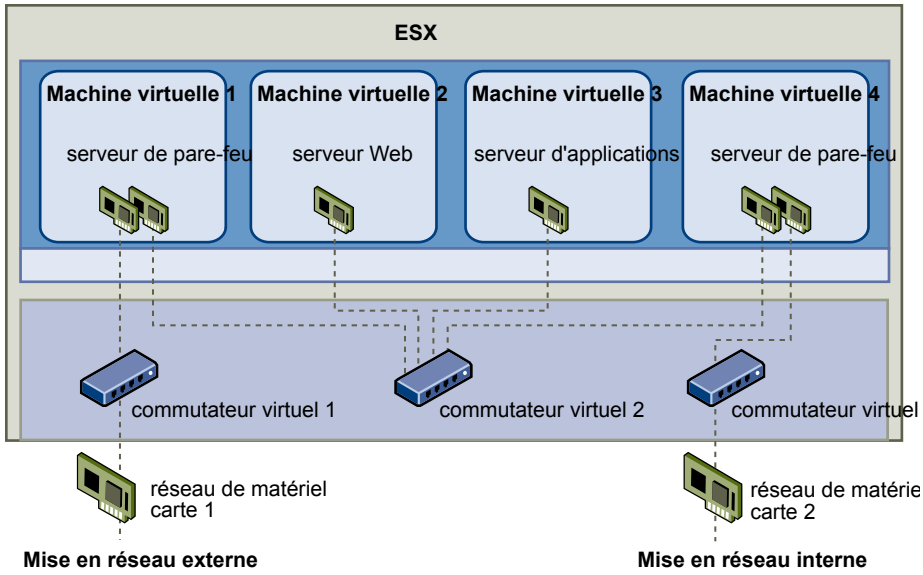
ESX prend également en charge les réseaux VLAN IEEE 802.1q, que vous pouvez utiliser pour renforcer la protection du réseau de machines virtuelles, la console de service ou la configuration de stockage. Les VLAN permettent de segmenter un réseau physique : ainsi, deux machines du même réseau physique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

Création d'une zone démilitarisée (DMZ) réseau sur un hôte ESX

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'ESX .

Figure 11-4 illustre cette configuration.

Figure 11-4. DMZ configurée sur un hôte ESX



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

- la machine virtuelle 1 et la machine virtuelle 4 sont équipées d'un pare-feu et sont connectées à des adaptateurs virtuels via des commutateurs virtuels. 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 virtuel 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 virtuel 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 virtuel situé au sein de la zone démilitarisée (commutateur virtuel 2). Puisque le serveur Web et le serveur d'applications sont également connectés à ce commutateur, ils peuvent traiter des requêtes externes.

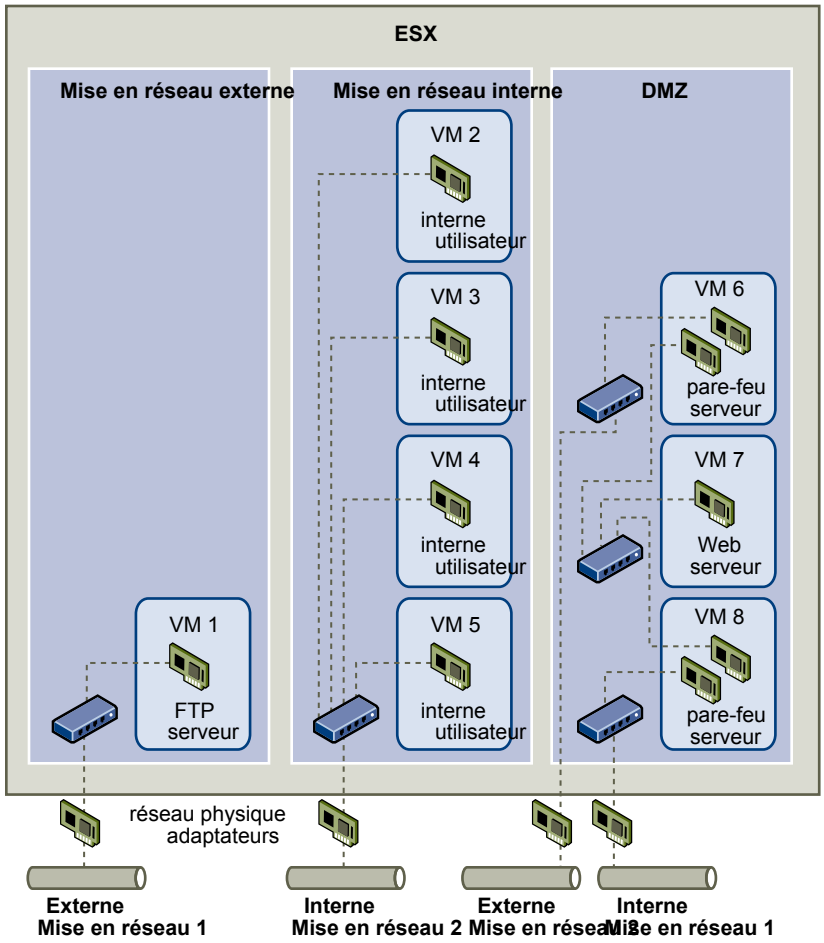
Le commutateur virtuel 2 est également connecté à la machine virtuelle 4. Cette machine virtuelle permet de bénéficier d'un pare-feu entre la DMZ et le réseau interne de l'entreprise. Ce pare-feu filtre les paquets en provenance du serveur Web et du serveur d'applications. Si un paquet est vérifié, il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

Le système ESX 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 11-5. Réseaux externes, réseaux internes et DMZ configurée sur un hôte ESX unique



Dans Figure 11-5, 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 ESX 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 groupes marketing les utilise pour publier le site Web externe de l'entreprise.

Ce groupes 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 groupes 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 ESX et être rassuré quant à l'absence de violations de données ou de ressources.

L'entreprise met en oeuvre 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 groupes.

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 ou dans vSphere Web Access.

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 ESX et des machines virtuelles en installant des pare-feu aux extrémités de la zone démilitarisée (DMZ), en vérifiant que l'hôte est protégé par un pare-feu physique et en configurant la console de service et les ressources de stockage réseau de telle sorte qu'elles bénéficient toutes de leur propre commutateur virtuel.

Sécurité et console de service

La console de service ESX est un produit Linux à distribution limitée, prenant comme base RHEL5 (Red Hat Enterprise Linux 5) La console de service offre un environnement d'exécution qui permet de surveiller et d'administrer l'hôte ESX.

Si la console de service est altérée, les machines virtuelles avec lesquelles elle est en interaction peuvent l'être également. Pour minimiser le risque d'attaque via la console de service, VMware protège cette console au moyen d'un pare-feu.

VMware utilise, outre ce pare-feu, différentes autres méthodes pour limiter les risques :

- ESX exécute uniquement les services nécessaires à la gestion de son fonctionnement, et la distribution est limitée aux fonctions requises pour l'exécution d'ESX.
- Par défaut, l'installation d'ESX comprend un niveau élevé de sécurité. Tous les ports sortants sont fermés et les seuls ports entrants ouverts sont ceux utilisés pour les interactions avec les clients (vSphere Client, par exemple). Vous devez conserver ce paramétrage, sauf si la console de service est connectée à un réseau de confiance.
- Par défaut, tous les ports non requis pour la gestion (accès à la console de service) 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 ESX utilisent SHA-1 avec chiffrement RSA en tant qu'algorithme de signature.
- Le service Web Tomcat (utilisé en interne par ESX par les clients Web tels que vSphere Web Access pour l'accès à la console de service) a été modifié : il exécute uniquement les fonctions requises pour les tâches d'administration et de surveillance effectuées par un client Web. Par conséquent, ESX 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 de la console de service ; en cas de besoin, un correctif de sécurité est envoyé, comme lors de tout autre problème de sécurité affectant les hôtes ESX. VMware fournit des correctifs de sécurité pour RHEL 5 et versions ultérieures, dès qu'elles sont disponibles sur le marché.

- 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 la console de service bénéficie d'un niveau suffisant de sécurité, vous devez dans ce cas ouvrir les ports correspondants.
- Le nombre d'applications utilisant un indicateur `setuid` ou `setgid` est minimisé. Vous pouvez mettre hors tension les applications `setuid` ou `setgid` qui ne sont pas nécessaires au bon fonctionnement d'ESX.

Même si vous pouvez installer et exécuter certains types d'applications conçues pour RHEL 5 sur la console de service, leur utilisation n'est prise en charge que si elle est explicitement confirmée par VMware. En cas de détection de vulnérabilité au sein d'une configuration prise en charge, VMware notifie de façon proactive tous les clients avec le support valide et les contacts d'abonnement, et les correctifs correspondants sont envoyés.

Remarque Suivez uniquement les instructions de sécurité fournies par VMware (vous les trouverez sur le site http://www.vmware.com/security/). Ne suivez pas les conseils de sécurité émis par Red Hat.

Ressources de sécurité et informations

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

Tableau 11-1 répertorie les rubriques liées à la sécurité et indique l'emplacement des informations complémentaires correspondantes.

Tableau 11-1. Ressources de sécurité VMware disponibles sur le Web

Rubrique	Ressources
Politique de sécurité VMware, alertes de sécurité actualisées, téléchargements de sécurité et discussions sur des thèmes liés à la sécurité	http://www.vmware.com/security/
Politique de l'entreprise en matière de réponse sécuritaire	http://www.vmware.com/support/policies/security_response.html VMware s'engage à vous aider à maintenir un environnement sécurisé. Dans ce cadre, les problèmes de sécurité sont corrigés rapidement. La politique VMware en matière de réponse sécuritaire fait état de notre engagement lié à la résolution d'éventuelles vulnérabilités de nos produits.
Politique de support logiciel tiers	http://www.vmware.com/support/policies/ VMware prend en charge un grand nombre de systèmes de stockage et d'agents logiciels (tels que les agents de sauvegarde ou les agents de gestion système). Vous trouverez la liste des agents, outils et autres logiciels ESX dans la rubriquehttp://www.vmware.com/vmtn/resources/ des guides de compatibilité ESX . 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.
Certification des produits VMware	http://www.vmware.com/security/certifications/
Information générale sur la virtualisation et la sécurité	Centre virtuel de ressources techniques de sécurité VMware http://www.vmware.com/go/security/

Tableau 11-1. Ressources de sécurité VMware disponibles sur le Web (suite)

Rubrique	Ressources
Standards de sécurité et de conformité, ainsi que solutions partenaires et contenu détaillé sur la virtualisation et la conformité	http://www.vmware.com/go/compliance/
Informations sur la technologie de protection de machines virtuelles VMsafe, incluant une liste de solutions partenaires	http://www.vmware.com/go/vmsafe/

Sécurisation d'une configuration ESX 12

Vous pouvez prendre des mesures pour promouvoir un environnement sécurisé pour vos hôtes ESX, 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.

Dans un environnement de machines virtuelles, vous pouvez planifier la disposition des pare-feu entre les composants.

- Les machines virtuelles telles que les hôtes vCenter Server et les hôtes ESX.
- 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 société).
- Une machine physique et une machine virtuelle, notamment lorsque vous placez un pare-feu entre un adapteur réseau physique et une machine virtuelle.

La manière dont vous utilisez des pare-feu dans une configuration ESX 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

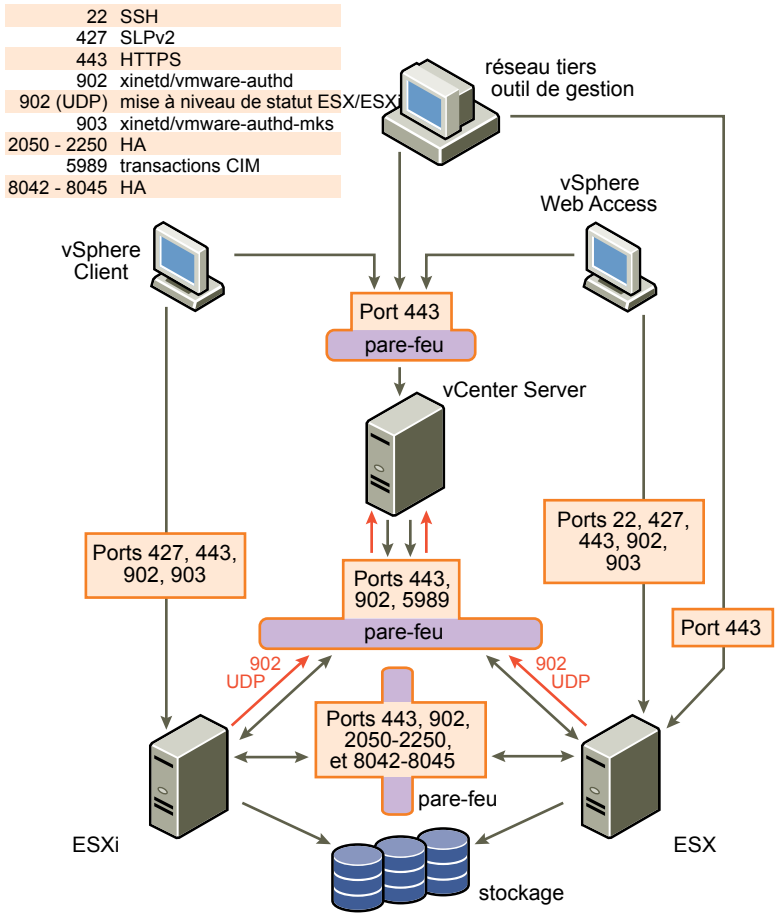
Si vous accédez aux hôtes ESX via vCenter Server, vous protégez généralement vCenter Server avec un pare-feu. Ce pare-feu fournit une protection de base à votre réseau.

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. Le point principal est de s'assurer qu'un pare-feu soit présent sur ce que vous considérez être un point d'entrée pour le système.

Si vous utilisez vCenter Server, vous pouvez installer des pare-feu à n'importe quel emplacement présenté dans Figure 12-1. En fonction de votre configuration, vous pouvez ne pas avoir besoin de tous les pare-feu de l'illustration, ou vous pouvez avoir besoin de pare-feu à d'autres emplacements. Par ailleurs, votre configuration peut comprendre des modules facultatifs, tels que VMware vCenter Update Manager, non représentés. Reportez-vous à la documentation pour plus d'informations sur les configurations de pare-feu spécifiques aux produits tels que Update Manager.

Pour obtenir la liste complète des ports TCP et UDP, y compris ceux pour VMware vMotion™ et Tolérance aux pannes VMware, voir « Ports TCP et UDP pour l'accès de gestion », page 171.

Figure 12-1. Exemple de configuration réseau vSphere et flux de trafic



Les réseaux configurés avec vCenter Server peuvent recevoir des communications via plusieurs types de clients : vSphere Client, vSphere Web Access 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 ESX. De nombreux emplacements de la liste et présentés dans Figure 12-1 sont facultatifs.

- Entre votre navigateur Web et le serveur proxy HTTP et HTTPS vSphere Web Access.
- Entre vSphere Client, vSphere Web Access Client ou un client de gestion réseau tiers et vCenter Server.
- Si vos utilisateurs accèdent aux machines virtuelles via vSphere Client, entre vSphere Client et l'hôte ESX. Cette connexion vient en plus de la connexion entre vSphere Client et vCenter Server et elle nécessite un port différent.
- Si vos utilisateurs accèdent aux machines virtuelles via un navigateur Web, entre le navigateur Web et l'hôte ESX. Cette connexion vient en plus de la connexion entre vSphere Web Access Client et vCenter Server et elle nécessite des ports différents.
- Entre vCenter Server et les hôtes ESX.
- Entre les hôtes ESX 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 sur les défaillances de sécurité de machine à machine.

  Si vous ajoutez des pare-feu entre les hôtes ESX 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 ESX et le stockage réseau tel que le stockage NFS et iSCSI. Ces ports ne sont pas spécifiques à VMware et vous pouvez les configurer en fonction des spécifications de votre réseau.

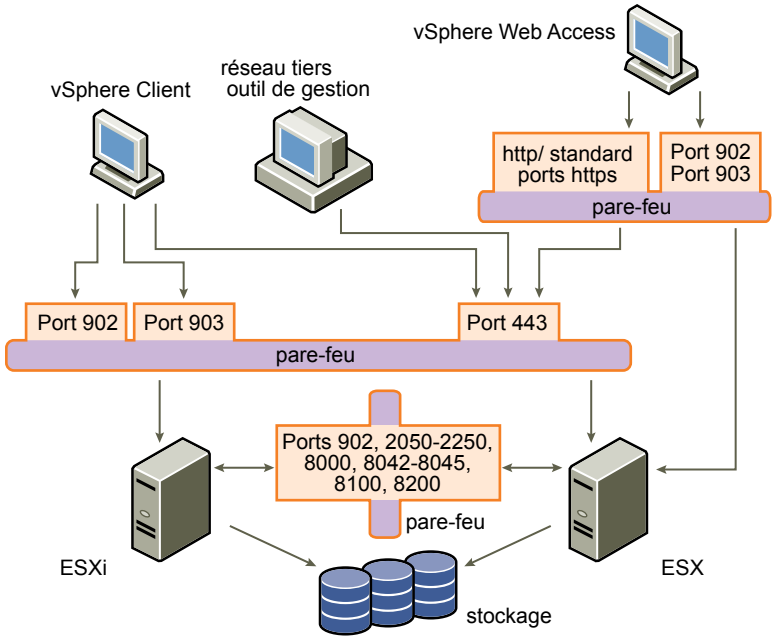
Pare-feux pour configurations sans vCenter Server

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

Vous pouvez installer des pare-feu à n'importe quel emplacement indiqué dans Figure 12-2.

Remarque En fonction de votre configuration, vous pouvez ne pas avoir besoin de tous les pare-feu de l'illustration, ou vous pouvez avoir besoin de pare-feu à des emplacements non représentés.

Figure 12-2. Configuration du pare-feu pour les réseaux ESX gérés directement par un client



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, clients de gestion de réseau tiers ou des clients vSphere Web Access. 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 ESX ou, en fonction de votre configuration, vos clients et votre couche ESX. 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 ESX 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 ESX 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, voir le *Guide d'administration du centre de données VMware vSphere*.

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

Lorsque vous connectez votre client à des hôtes ESX 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 ESX et utilisent différents protocoles d'authentification.

Port 902

vCenter Server utilise ce port pour envoyer des données aux hôtes gérés de vCenter Server. Le port 902 est le port que vCenter Server considère comme disponible lors de l'envoi de données à un hôte ESX.

Le port 902 connecte vCenter Server à l'hôte via le démon agréé VMware (`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, vSphere Web Access Client et SDK utilisent ce port pour envoyer des données aux hôtes gérés par vCenter Server. Par conséquent, vSphere Client, vSphere Web Access Client et SDK, s'ils sont connectés directement à un hôte ESX, 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 l'hôte ESX. VMware ne prend pas en charge la configuration d'un port différent pour ces connexions.

Le port 443 connecte les clients à l'hôte ESX via le service Web Tomcat ou SDK. `vmware-hostd` multiplexe les données du port 443 au destinataire approprié pour le traitement.

Port 903

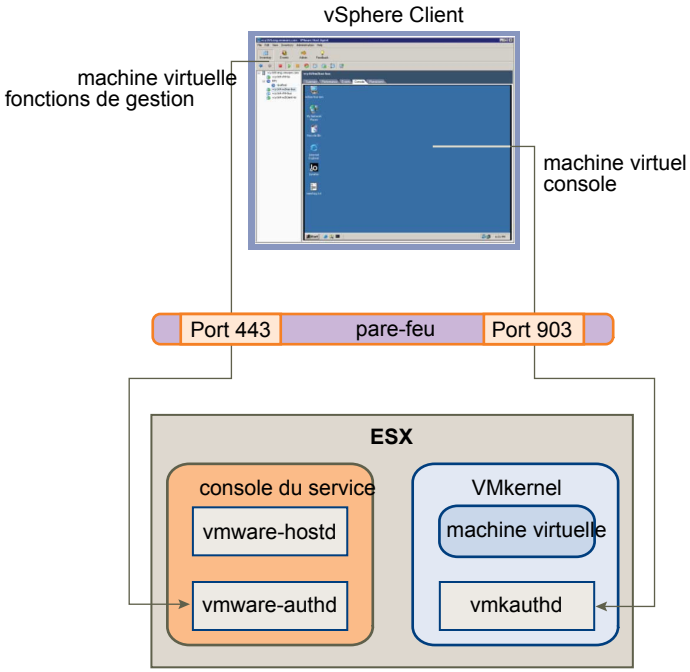
vSphere Client et vSphere Web Access utilisent ce port pour fournir une connexion pour les activités MKS du système d'exploitation invité sur les machines virtuelles. C'est par ce port que les utilisateurs interagissent avec les systèmes d'exploitation et les applications invités de la machine virtuelle. Le port 903 est le port que vSphere Client et vSphere Web Access considèrent 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 l'hôte ESX.

Figure 12-3 présente les relations entre les fonctions de vSphere Client, les ports et les processus ESX.

vSphere Web Access Client utilise le même mappage de base pour ses interactions avec l'hôte ESX.

Figure 12-3. Utilisation des ports pour les communications client avec ESX



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

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

Connexion des hôtes ESX via les pare-feu

Si un pare-feu se trouve entre deux hôtes ESX et que vous souhaitiez autoriser des transactions entre les hôtes ou utiliser vCenter Server pour effectuer des activités source ou cible, telles que du trafic VMware High Availability (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 des ports dans les plages suivantes :

- 443 (migration serveur à serveur et trafic d'approvisionnement)
- 2050–2250 (pour le trafic HA)
- 8000 (pour vMotion)
- 8042-8045 (pour le trafic HA)

Consultez l'administrateur système du pare-feu pour plus d'informations sur la configuration des ports.

Configuration des ports pare-feu pour les services pris en charge et les agents de gestion

Vous devez configurer les pare-feu dans votre environnement pour accepter les services pris en charge les plus courants.

Utilisez vSphere Client pour configurer le pare-feu de la console du service. Lorsque vous configurez le profil de sécurité de l'hôte ESX dans vCenter Server, vous ajoutez ou supprimez ces services ou agents, en ouvrant ou en fermant automatiquement des ports prédéterminés dans le pare-feu pour permettre la communication avec le service ou l'agent.

Les services et agents suivants sont généralement présents dans un environnement vSphere :

- client NFS (service non sécurisé)
- Client NTP
- client logiciel iSCSI
- serveur HTTP CIM (service non sécurisé)
- serveur HTTPS CIM
- client Syslog
- serveur NFS (service non sécurisé)
- client NIS
- client SMB (service non sécurisé)
- client FTP (service non sécurisé)
- client SSH
- client Telnet (service non sécurisé)
- serveur SSH
- serveur Telnet (service non sécurisé)
- serveur FTP (service non sécurisé)
- serveur SNMP
- Autres agents de gestion pris en charge installés

Remarque La liste peut évoluer. Par conséquent, il se peut que vSphere Client fournisse des services et des agents non répertoriés dans la liste. Tous les services indiqués dans la liste ne sont également pas installés par défaut. Vous pouvez être invité à effectuer des tâches supplémentaires pour configurer et activer ces services.

Si vous installez un périphérique, un service ou un agent ne figurant pas sur la liste, ouvrez les ports dans le pare-feu de la console du service à partir d'une ligne de commande.

Autorisation d'accès à l'ESX pour un service ou un agent de gestion

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

Procédure

1 Ouvrez une session sur un système vCenter Server au moyen de 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 Cliquez sur **[Propriétés]** pour ouvrir la boîte de dialogue Propriétés de pare-feu.

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

5 Sélectionnez les services et les agents à activer.

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]** .

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

ESX 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'utilitaire `esxcfg-firewall` ou les fichiers de configuration se trouvant dans `/etc/init.d/`, ne se trouvent pas affectées par ces paramètres.

- **[Démarrer automatiquement si ports ouverts, et arrêter quand tous ports fermés]** : 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.
- **[Démarrer et arrêter avec 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.

Configuration de la relation entre démarrage de service et configuration de pare-feu

La stratégie de démarrage détermine le moment auquel un service démarre. Vous pouvez configurer la relation entre le démarrage d'un service et la configuration du pare-feu en éditant la stratégie de démarrage.

Procédure

1 Ouvrez une session sur un système vCenter Server au moyen de 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 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 à gérer 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]** .

Ports TCP et UDP pour l'accès de gestion

vCenter Server, les hôtes ESX 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.

Tableau 12-1 répertorie les ports TCP et UDP et l'objectif et le type de chaque port.

Les ports sont connectés via l'interface de la console du service, sauf mention contraire.

Tableau 12-1. Ports TCP et UDP

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

Tableau 12-1. 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 ESX. Accès vSphere Client aux consoles des machines virtuelles Accès vSphere Web Access Client aux consoles des machines virtuelles Transactions MKS (xinetd/vmware-authd-mks)	TCP entrant
2049	Transactions provenant des périphériques de stockage NFS Ce port est utilisé sur l'interface VMkernel plutôt que sur l'interface de la console du service.	UDP entrant et sortant
2050–2250	Trafic entre les hôtes ESX pour VMware High Availability (HA) et EMC Autostart Manager	TCP sortant, UDP entrant et sortant
3260	Transactions vers les périphériques de stockage iSCSI Ce port est utilisé sur l'interface VMkernel et sur l'interface de la console du service.	TCP sortant
5900-5964	Protocole RFB qui est utilisé par les outils de gestion tels que VNC	UDP entrant et sortant
5989	Transactions XML CIM sur HTTPS	UDP entrant et sortant
8000	Requêtes de vMotion Ce port est utilisé sur l'interface VMkernel plutôt que sur l'interface de la console du service.	UDP entrant et sortant
8042–8045	Trafic entre les hôtes ESX pour HA et EMC Autostart Manager	TCP sortant, UDP entrant et sortant
8100, 8200	Trafic entre les hôtes ESX pour Tolérance aux pannes VMware	TCP sortant, UDP entrant et sortant

En plus des ports TCP et UDP répertoriés dans Tableau 12-1, vous pouvez configurer d'autres ports en fonction de vos besoins :

- Vous pouvez utiliser vSphere Client afin d'ouvrir des ports pour les agents de gestion installés et les services pris en charge tels que NFS.
- Vous pouvez ouvrir des ports dans le pare-feu de la console du service pour d'autres services et agents requis pour votre réseau en exécutant des scripts de ligne de commande.

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.

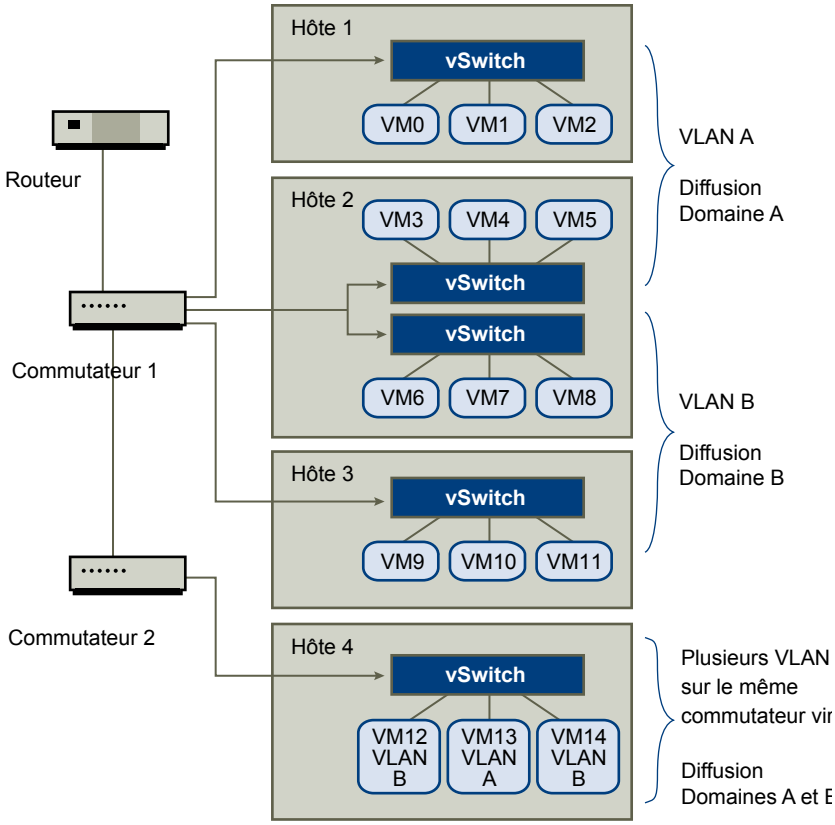
  La planification soignée de la segmentation réduit les chances de transmissions de paquets entre les zones de machines virtuelles, ce qui empêche les attaques de reniflement qui nécessitent l'envoi de trafic réseau à la victime. Par conséquent, un attaquant ne peut pas utiliser un service non sécurisé 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 comme indiqué dans Figure 12-4.

Figure 12-4. 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.

ESX 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 niveau 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 virtuels VWware 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 virtuels 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.

Création de communications séparées entre les outils de gestion et la console du service

Que vous utilisiez un client de gestion ou la ligne de commande, toutes les tâches de configuration de l'ESX sont effectuées via la console du service, y compris la configuration du stockage, le contrôle des aspects du comportement de la machine virtuelle et la configuration des commutateurs virtuels ou des réseaux virtuels. Comme la console du service est le point de contrôle de l'ESX, la préserver d'une utilisation incorrecte est crucial.

Les clients de gestion ESX de VMware utilisent l'authentification et le chiffrement pour empêcher tout accès non autorisé à la console du service. D'autres services peuvent ne pas présenter la même protection. Si des attaquants parviennent à accéder à la console du service, ils sont libres de reconfigurer de nombreux attributs de l'hôte ESX. Par exemple, ils peuvent modifier toute la configuration des commutateurs virtuels ou modifier les méthodes d'autorisation.

La connectivité réseau pour la console du service est établie via les commutateurs virtuels. Pour améliorer la protection de ce composant ESX critique, isolez la console du service en utilisant l'une des méthodes suivantes :

- Créez un VLAN séparé pour la communication des outils de gestion avec la console du service.
- Configurez l'accès réseau pour les connexions des outils de gestion avec la console du service via un seul commutateur virtuel ou un ou plusieurs ports de liaison montante.

Les deux méthodes empêchent toute personne n'accédant pas à la console du service ou au commutateur virtuel de voir le trafic provenant de et allant vers la console du service. Elles empêchent également les attaquants d'envoyer des paquets à la console du service. Vous pouvez également configurer la console du service sur un segment de réseau physique séparé. La segmentation physique fournit un degré de sécurité supplémentaire, car elle est moins sujette à une configuration incorrecte ultérieure.

Configurez un VLAN séparé ou un commutateur virtuel pour vMotion et un stockage lié au réseau.

Protection des commutateurs virtuels et VLAN

Les commutateurs virtuels VMware assurent une protection contre certaines menaces à la sécurité du VLAN. En raison de la manière dont certaines machines virtuelles sont conçues, 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 virtuels ne protègent pas le réseau physique contre ces attaques : ils protègent uniquement le réseau virtuel.

Les commutateurs virtuels 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 (CAM) 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 virtuels 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 virtuels de VMware n'effectuent pas le tronçonnage dynamique requis 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 virtuels 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 virtuels 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 virtuels 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 virtuels 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 virtuels

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 virtuel pour votre réseau, vous ajoutez des groupes de ports pour imposer une configuration des 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 groupes de ports à un commutateur virtuel, vSphere Client configure un profil de sécurité pour le port. Vous pouvez utiliser ce profil de sécurité pour garantir que ESX 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 virtuel sur les hôtes ESX 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 virtuel 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]** , ESX 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]** , ESX 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 ESX 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.

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]** , ESX 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, ESX 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 ESX 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 virtuel 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 ESX supportent 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.

IPsec et IPv6 sur la console de service ne sont pas pris en charge.

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 vSphere CLI. Pour plus d'informations sur l'utilisation de vSphere CLI, voir le *Guide d'installation et script de l'interface de ligne de commande vSphere* et le *Référence de l'interface de ligne de commande vSphere*.

Procédure

1 Utilisez la commande `esxcfg-ipsec --add-sa`.

2 Définissez l'adresse source à l'aide de `--sa-src adresse source`.

3 Définissez l'adresse de destination à l'aide de `--sa-dst adresse destination`.

4 Choisissez le mode, soit `transport` ou `tunnel` à l'aide du `mode --sa-mode .`

5 Indiquez l'index des paramètres de sécurité à l'aide de `--spi index des paramètres de sécurité`.

L'index des paramètres de sécurité 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.

6 Choisissez l'algorithme de chiffrement à l'aide de `--ealgo algorithme de chiffrement`.

- `3des-cbc`
- `aes128-cbc`
- `null` ne fournit aucun chiffrement

7 Choisissez la clé de chiffrement à l'aide de `--ealgo clé de chiffrement`.

Vous pouvez entrer des clés en tant que texte ASCII ou en tant qu'hexadécimal avec un préfixe 0x.

8 Choisissez l'algorithme d'authentification, `hmac-sha1` ou `hmac-sha2-256` à l'aide de `--ialgo authentication algorithm`.

9 Fournissez la clé d'authentification à l'aide de `--ealgo clé d'authentification`.

Vous pouvez entrer des clés en tant que texte ASCII ou en tant qu'hexadécimal avec un préfixe 0x.

10 Fournissez un nom à l'association de sécurité à l'aide de `nom`.

Exemple 12-1. Exemple de commande de nouvelle association de sécurité

L'exemple suivant contient des sauts de ligne supplémentaires pour des raisons de lisibilité.

```
esxcfg-ipsec --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 ESX.

Vous pouvez supprimer une association de sécurité à l'aide de vSphere CLI. Pour plus d'informations sur l'utilisation de vSphere CLI, voir le *Guide d'installation et script de l'interface de ligne de commande vSphere* et le *Référence de l'interface 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.

Procédure

- Utilisez la commande `esxcfg-ipsec --remove-sa security association name`.

Liste des associations de sécurité disponibles

ESX 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 vSphere CLI. Pour plus d'informations sur l'utilisation de vSphere CLI, voir le *Guide d'installation et script de l'interface de ligne de commande vSphere* et le *Référence de l'interface de ligne de commande vSphere*.

Procédure

- Utilisez la commande `esxcfg-ipsec -l`.

ESX 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 vSphere CLI. Pour plus d'informations sur l'utilisation de vSphere CLI, voir le *Guide d'installation et script de l'interface de ligne de commande vSphere* et le *Référence de l'interface de ligne de commande vSphere*.

Prérequis

Avant de créer une règle de sécurité, ajoutez une association de sécurité avec les paramètres d'authentification et de chiffrement appropriés.

Procédure

1. Utilisez la commande `esxcfg-ipsec --add-sp`.
2. Définissez l'adresse IP source et la longueur de préfixe à l'aide de `--sp-src adresse source`.
3. Définissez l'adresse de destination et la longueur de préfixe à l'aide de `--sp-dst adresse destination`.
4. Définissez le port source à l'aide de `--src-port port`.

   Le port source doit être un nombre compris entre 0 et 65 535.
5. Définissez le port de destination à l'aide de `--dst-port port`.

   Le port de destination doit être un nombre compris entre 0 et 65 535.
6. Choisissez le protocole de couche supérieure à l'aide de `--ulproto protocole`.
   - `tcp`
   - `udp`
   - `icmp6`
   - `toutes`
7. Choisissez la direction, `in` ou `out`, dans laquelle vous souhaitez surveiller le trafic à l'aide de `--dir direction`.

8 Définissez l'action à prendre lorsque le trafic avec les paramètres spécifiés est rencontré à l'aide de `--action action`.

Option	Description
aucune	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.

9 Choisissez le mode, soit `tunnel` ou `transport` à l'aide de `--sp-mode mode`.

10 Définissez l'association de sécurité pour cette règle de sécurité à utiliser à l'aide de `--sa-name nom association de sécurité`.

11 Définissez le nom de la règle de sécurité à l'aide de `nom`.

Exemple 12-2. Exemple de commande de nouvelle règle de sécurité

L'exemple suivant contient des sauts de ligne supplémentaires pour des raisons de lisibilité.

```
esxcfg-ipsec --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 ESX.

Vous pouvez supprimer une règle de sécurité à l'aide de vSphere CLI. Pour plus d'informations sur l'utilisation de vSphere CLI, voir le *Guide d'installation et script de l'interface de ligne de commande vSphere* et le *Référence de l'interface 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.

Procédure

- Utilisez la commande `esxcfg-ipsec --remove-sp security policy name`.

Liste des règles de sécurité disponibles

ESX peuvent 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 vSphere CLI. Pour plus d'informations sur l'utilisation de vSphere CLI, voir le *Guide d'installation et script de l'interface de ligne de commande vSphere* et la *Référence de l'interface de ligne de commande vSphere*.

Procédure

- Utilisez la commande `esxcfg-ipsec -L`.

ESX affiche une liste de toutes les règles de sécurité disponibles.

Sécurisation du stockage iSCSI

Le stockage que vous configurez pour un hôte ESX peut comprendre un ou plusieurs réseaux de zone de stockage (SAN) utilisant iSCSI. Lorsque vous configurez iSCSI sur un hôte ESX, 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 ESX 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 ESX et à celles des iSCSI configurés directement via l'hôte ESX.

Sécurisation des périphériques iSCSI via l'authentification

Un moyen permettant de sécuriser les périphériques iSCSI des intrusions indésirables consiste à demander que l'hôte ESX, 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.

ESX 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.

ESX 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.

ESX 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.

Voir « Configurer des paramètres CHAP pour des cartes iSCSI », page 109 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.

Voir « Configurer des paramètres CHAP pour des cartes iSCSI », page 109 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

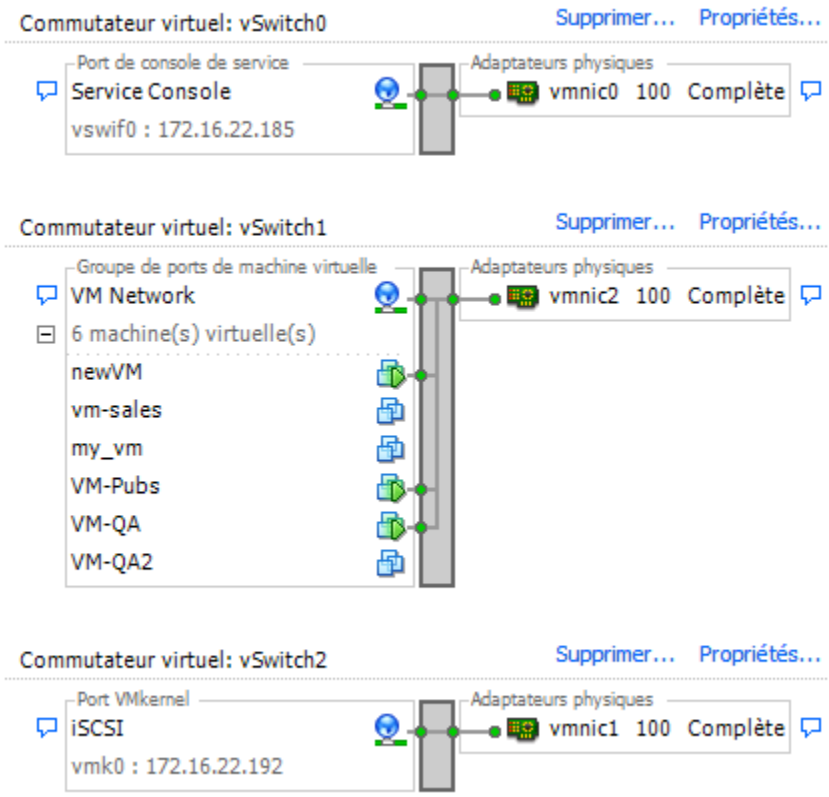
Le premier risque de sécurité dans les SAN iSCSI est qu'un attaquant puisse renifler les données de stockage transmises.

Prenez des mesures supplémentaires pour empêcher les attaquants de voir aisément les données iSCSI. Ni l'adaptateur iSCSI du matériel, ni l'initiateur iSCSI de l'hôte ESX ne chiffre les données qu'ils transmettent vers les cibles et obtiennent de celles-ci, rendant ainsi les données plus vulnérables aux attaques par renifflage.

Permettre à vos machines virtuelles de partager des commutateurs virtuels 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 ESX 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 ESX, vous pouvez effectuer cette opération en configurant le stockage iSCSI via un commutateur virtuel différent de celui utilisé par vos machines virtuelles, comme indiqué dans Figure 12-5.

Figure 12-5. Stockage iSCSI sur un commutateur virtuel séparé



En plus de protéger le SAN iSCSI en lui attribuant un commutateur virtuel, 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, l'hôte ESX n'ouvre pas de port écoutant les connexions réseau. Cette mesure réduit les chances qu'un intrus puisse pénétrer dans l'hôte ESX 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 ESX 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'un défaut ESX. 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.

Authentification et gestion d'utilisateurs 13

ESX 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 ESX via l'authentification et les autorisations

Lorsqu'un utilisateur du vSphere Client ou de vCenter Server se connecte à l'hôte ESX, 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.

ESX utilise la structure PAM (Pluggable Authentication Modules) pour effectuer une authentification quand les utilisateurs accèdent à l'hôte ESX via le vSphere Client, vShpere Web Access ou la console de service. La configuration PAM pour les services VMware se trouve dans `/etc/pam.d/vmware-authd` où sont stockés les chemins d'accès aux modules d'authentification.

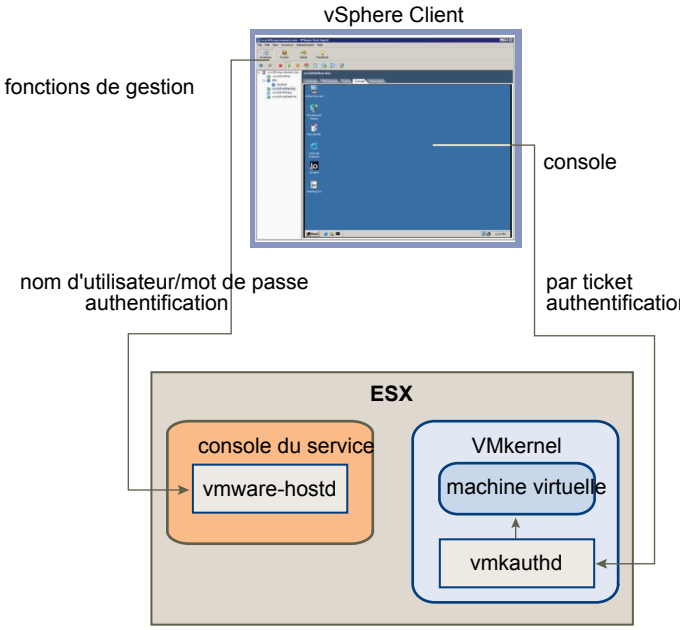
L'installation ESX par défaut utilise l'authentification `/etc/passwd` tout comme Linux, mais vous pouvez configurer ESX de manière à utiliser un autre mécanisme d'authentification distribué. Si vous prévoyez d'utiliser un outil d'authentification tiers au lieu de l'implémentation ESX par défaut, consultez la documentation du fabricant pour obtenir des instructions. Lors de la configuration de l'authentification tierce, vous devez peut-être mettre à niveau les fichiers dans le dossier `/etc/pam.d` avec les nouvelles informations de module.

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

Figure 13-1 montre un exemple basique d'authentification des transactions par ESX depuis le vSphere Client.

Remarque Les transactions CIM utilisent également l'authentification par ticket en se connectant avec le processus `vmware-hostd`.

Figure 13-1. Authentification des communications du vSphere Client avec ESX



Les transactions d'authentification ESX avec vSphere Web Access et des clients de gestion réseau tiers sont aussi des transactions directes avec le processus `vmware-hostd`.

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.

À propos des utilisateurs, des groupes, des autorisations et des rôles

vCenter Server et les hôtes ESX emploient le nom d'utilisateur, le mot de passe et les autorisations pour authentifier l'accès d'un utilisateur ou autoriser des activités. Vous pouvez contrôler l'accès à des hôtes, clusters, banque de données, pools de ressources, groupes de ports réseau et machines virtuelles en attribuant des autorisations.

L'accès à un hôte ESX et à ses ressources est accordé lorsqu'un utilisateur connu disposant des autorisations adéquates ouvre une session sur l'hôte avec un mot de passe correct. vCenter Server utilise une approche similaire lorsqu'il décide d'accorder l'accès à un utilisateur.

vCenter Server et les hôtes ESX refusent l'accès dans les circonstances suivantes :

- Un utilisateur non répertorié dans la liste d'utilisateurs tente d'ouvrir une session.
- Un utilisateur saisit le mauvais mot de passe.
- Un utilisateur fait partie de la liste mais ne dispose pas des autorisations attribuées.
- Un utilisateur ayant réussi à ouvrir une session tente d'effectuer des opérations pour lesquelles il ne possède pas les autorisations.

Lors de la gestion des hôtes ESX et de vCenter Server, vous devez prévoir la gestion de types d'utilisateur et d'autorisations spécifiques. ESX et vCenter Server utilisent des ensembles de privilèges ou des rôles pour contrôler les opérations que peuvent exécuter les groupes ou utilisateurs individuels. Des rôles prédéfinis sont fournis, mais vous pouvez également en créer de nouveaux. Vous pouvez gérer plus facilement des utilisateurs en leur attribuant des groupes. Lorsque vous appliquez un rôle à un groupes, tous les utilisateurs de ce groupes héritent du rôle.

Les sujets de cette section s'appliquent aux utilisateurs et groupes de travail locaux. Vous pouvez également utiliser Active Directory pour gérer les utilisateurs et groupes pour ESX.

Comprendre les utilisateurs

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

Les utilisateurs ESX 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, vSphere Web Access, 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 un hôte ESX 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 ESX gère localement se distingue des utilisateurs connus par vCenter Server, ces derniers étant des utilisateurs Windows locaux ou faisant partie du domaine Windows. Même si la liste semble contenir des utilisateurs communs (par exemple, un utilisateur appelé devuser), traitez ces utilisateurs séparément. Si vous ouvrez une session vCenter Server en tant que devuser, vous disposez peut-être d'une autorisation pour afficher et supprimer des fichiers depuis une banque de données ; ce n'est peut-être pas le cas si vous ouvrez une session de l'hôte ESX en tant que devuser. 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 ESX.

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 ESX pour éviter les doublons. Pour contrôler les utilisateurs de vCenter Server, consultez la liste de domaine Windows.

Comprendre les groupes

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

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 groupes 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.

Les listes de groupes dans vCenter Server et un hôte ESX 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 ESX proviennent de la liste d'utilisateurs locaux ou de tout domaine Windows approuvé.

Comprendre les conditions d'un mot de passe

Par défaut, ESX 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 13-1. Exemple de mots de passe

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

- 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 d'ESX.

- 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.

Comprendre les autorisations

Pour ESX 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 ESX.

La capacité de la plupart des utilisateurs du vCenter Server et d'ESX à manipuler les objets associés à l'hôte est limitée. Les utilisateurs disposant du rôle administrateur ont des autorisations et droits d'accès complets sur tous les objets virtuels tels que des banque de données, des hôtes, des machines virtuelles et des pools de ressources. Par défaut, le rôle Administrateur est accordé à l'utilisateur racine. Si vCenter Server gère l'hôte, vpxuser est également un utilisateur Administrateur.

La liste de privilèges est la même pour ESX 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 ESX. Ces tâches étant largement exécutées dans vCenter Server, consultez le *guide d'administration du centre de données VMware vSphere* pour plus d'informations sur l'utilisation des autorisations et rôles.

Attribuer des autorisations à l'utilisateur racine

Les utilisateurs racines peuvent uniquement effectuer des actions sur l'hôte ESX 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 le vSphere Client, comme indiqué dans le *Guide d'administration de centre de données VMware vSphere*. 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 groupes d'utilisateurs ou utilisateur différent) vous pouvez suivre les actions de chaque administrateur ou groupes 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.

Comprendre les autorisations de vpxuser

L'autorisation de vpxuser est utilisée par le vCenter Server pour gérer les activités de l'hôte. vpxuser est créé lorsqu'un hôte ESX est relié au vCenter Server.

vCenter Server possède des privilèges 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 ESX. Ces tâches peuvent uniquement être exécutées par un utilisateur disposant des autorisations Administrateur directement sur chaque hôte ESX.

Remarque Vous ne pouvez pas gérer vpxuser via Active Directory.

Avertissement Ne modifiez en aucun cas vpxuser et ne changez pas ses autorisations. Dans le cas contraire, vous risquez d'avoir des difficultés à utiliser des hôtes ESX via vCenter Server.

Comprendre les rôles

vCenter Server et ESX 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 ESX 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 le vSphere Client connecté au vCenter Server afin de gérer vos hôtes ESX, vous disposez de choix de rôles supplémentaires dans vCenter Server. Par ailleurs, les rôles que vous créez directement sur un hôte ESX 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 le vSphere Client.

Si vous gérez des hôtes ESX 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 ESX. Étant donné que la plupart des utilisateurs créent des rôles et configurent des autorisations dans vCenter Server, consultez le *Guide d'administration du centre de données VMware vSphere* pour plus d'informations sur l'utilisation des autorisations et rôles.

Attribuer le rôle aucun accès

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

Les autorisations d'utilisateur vpxuser et d'utilisateur racine sont les seuls utilisateurs non assignés au rôle Aucun accès par défaut. Ils sont en revanche assignés au rôle Administrateur. Vous pouvez entièrement supprimer les autorisations de l'utilisateur racine ou lui octroyer le rôle Aucun accès du moment que vous créez en premier lieu une autorisation de remplacement au niveau de la racine avec le rôle Administrateur et associez ce rôle à un autre utilisateur.

Attribuer le rôle Lecture seule

Les utilisateurs assignés aux rôle Lecture seule pour un objet sont autorisés à afficher l'état et les détails de l'objet.

Grâce à ce rôle, un utilisateur peut afficher les caractéristiques d'une machine virtuelle, d'un hôte et d'un pool de ressources. L'utilisateur ne peut pas voir la console à distance pour un hôte. Toutes les actions via les menus et barres d'outils ne sont pas autorisées.

Attribuer le rôle Administrateur

Les utilisateurs assignés au rôle Administrateur pour un objet sont autorisés à afficher et à exécuter toutes les actions sur cet objet. Ce rôle comprend également toutes les autorisations inhérentes au rôle Lecture seule.

Si vous disposez du rôle Administrateur sur un hôte ESX, vous pouvez accorder des autorisations à des groupes et utilisateurs individuels sur cet hôte. Si vous disposez du rôle Administrateur dans vCenter Server, vous pouvez accorder des autorisations à tout groupes ou utilisateur inclus dans la liste de domaine Windows référencée par vCenter Server.

vCenter Server inscrit tout groupes ou utilisateur de domaine Windows sélectionné via le processus d'attribution des autorisations. Par défaut, tous les utilisateurs membres du groupes d'administrateurs Windows locaux sur vCenter Server reçoivent les mêmes droits d'accès que l'utilisateur assigné au rôle Administrateur. Les utilisateurs membres du groupes Administrateurs peuvent ouvrir une session en tant qu'individus et disposer d'un accès complet.

Les utilisateurs du groupe Active Directory ESX Admins reçoivent automatiquement le rôle d'Administrateur.

Pour des raisons de sécurité, envisagez de supprimer le groupes Administrateurs Windows du rôle Administrateur. Vous pouvez modifier les autorisations après l'installation. Vous pouvez également utiliser le vSphere Client pour supprimer les autorisations d'accès du groupes Administrateurs Windows, mais vous devez d'abord créer au niveau de la racine une autre autorisation avec un utilisateur différent assigné au rôle Administrateur.

Travailler avec des utilisateurs et groupes sur des hôtes ESX

Si vous êtes directement connecté à un hôte ESX via le vSphere Client, vous pouvez créer, modifier et supprimer des utilisateurs et groupes. Ces utilisateurs ou groupes sont visibles dans vSphere Client à chaque fois que vous ouvrez une session de l'hôte ESX, mais ne sont pas disponibles lorsque vous ouvrez une session du vCenter Server.

Les sujets de cette section s'appliquent aux utilisateurs et groupes de travail locaux. Vous pouvez également utiliser Active Directory pour gérer les utilisateurs et groupes pour ESX.

Afficher, trier et exporter une liste d'utilisateurs et de groupes

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

Procédure

1 Ouvrez une session de l'hôte avec le vSphere Client.

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

Ajouter un utilisateur au tableau d'utilisateurs

Ajouter un utilisateur au tableau d'utilisateurs met à niveau la liste d'utilisateurs interne conservée par ESX.

Prérequis

Passez en revue les exigences de mot de passe décrites dans « Comprendre les conditions d'un mot de passe », page 190.

Procédure

1 Ouvrez une session de l'hôte avec le vSphere Client.

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

- 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`.
- Si vous avez basculé sur le plug-in d'authentification `pam_cracklib.so`, la conformité du mot de passe n'est pas appliquée.

5 Pour autoriser un utilisateur à accéder à l'hôte ESX via une invite de commande, sélectionnez **[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 groupes, sélectionnez le nom du groupes dans le menu déroulant **[groupes]** , puis cliquez sur **[Ajouter]** .

7 Cliquez sur **[OK]** .

Modifier les paramètres pour un utilisateur

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 « Comprendre les conditions d'un mot de passe », page 190.

Procédure

1 Ouvrez une session de l'hôte avec le vSphere Client.

2 Cliquez sur l'onglet **[Utilisateurs et groupes]** , puis 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 modifier le mot de passe utilisateur, sélectionnez **[Changer mot 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`.
- Si vous avez basculé sur le plug-in d'authentification `pam_cracklib.so`, la conformité du mot de passe n'est pas appliquée.

7 Pour modifier l'accès de l'utilisateur à l'hôte ESX via le shell de commande, sélectionnez **[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 groupes, sélectionnez le nom du groupes dans le menu déroulant **[groupes]** , puis cliquez sur **[Ajouter]** .

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

10 Cliquez sur **[OK]** .

Supprimer un utilisateur ou groupes

Vous pouvez supprimer un utilisateur ou groupes de l'hôte ESX.

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.

La suppression d'un groupes 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 groupes.

Procédure

1 Ouvrez une session de l'hôte avec le vSphere Client.

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

3 Cliquez avec le bouton droit sur l'utilisateur ou groupes que vous voulez supprimer, puis sélectionnez **[Supprimer]** .

Ajouter un groupes au tableau de groupes

Ajouter un groupes au tableau de groupes d'ESX met à niveau la liste de groupes interne conservée par l'hôte.

Procédure

1 Ouvrez une session de l'hôte avec le vSphere Client.

2 Cliquez sur l'onglet **[Utilisateurs et groupes]** , puis 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 Tapez un nom de groupes et un ID de groupes numérique (GID) dans la zone de texte **[ID groupes]** .

La saisie du GID est facultative. Si vous ne spécifiez pas de GID, le vSphere Client attribue le prochain ID de groupes disponible.

5 Pour chaque utilisateur que vous voulez ajouter comme membre du groupes, sélectionnez le nom d'utilisateur dans la liste et cliquez sur **[Ajouter]** .

6 Cliquez sur **[OK]** .

Ajouter ou supprimer des utilisateurs d'un groupes

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

Procédure

1 Ouvrez une session de l'hôte avec le vSphere Client.

2 Cliquez sur l'onglet **[Utilisateurs et groupes]** , puis 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 groupes, sélectionnez le nom du groupes dans le menu déroulant **[groupes]** , puis cliquez sur **[Ajouter]** .

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

6 Cliquez sur **[OK]** .

Configurer un hôte pour utiliser un service d'annuaire

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

Prérequis

Vérifiez que vous avez installé un domaine Active Directory. Reportez-vous à la documentation de votre serveur d'annuaire.

Procédure

1 Assurez-vous que le nom d'hôte d'ESX est pleinement qualifié par le nom de domaine de la forêt Active Directory.

fully qualified domain name = host_name.domain_name

2 Synchronisez l'heure entre ESX et le système de service d'annuaire en utilisant votre méthode préférée.

Pour utiliser NTP, suivez les étapes suivantes.

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

b Cliquez sur l'onglet **[Configuration]** et cliquez sur **[Configuration de temps]** .

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

d Définissez la date et l'heure.

e Sélectionnez **[Client NTP activé]** pour ouvrir les ports de pare-feu de console du service que le service NTP utilise.

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

Vous pouvez utiliser la boîte de dialogue de Configuration de Routage et vSphere Client DNS pour modifier le nom de l'hôte et les informations de serveur DNS pour l'hôte.

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 pour accéder à la boîte de dialogue Configuration Routage et DNS.

Suivant

Joignez un domaine de service d'annuaire en utilisant le vSphere Client.

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.

Prérequis

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

Procédure

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

2 Sous Logiciel, cliquez sur **[Services d'authentification]** et cliquez sur **[Propriétés]** .

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

Option	Description
Si vous choisissez Active Directory	Entrez un domaine sous la forme **`name.tld`** ou **`name.tld/container/path`** et cliquez sur **[Joindre le domaine]** .
Si l'hôte utilise déjà un service d'annuaire	Sélectionnez **[Quitter domaine]** pour quitter le domaine et en rejoindre un autre.

4 Saisissez le nom d'utilisateur et mot de passe d'un utilisateur Active Directory autorisé à joindre l'hôte au domaine, puis cliquez sur **[OK]** .

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

Utiliser des profils d'hôte pour appliquer des autorisations aux hôtes

Lorsque vous joignez un hôte à un domaine Active Directory, vous devez définir des rôles sur l'hôte pour un utilisateur ou groupes dans ce domaine. Sinon, l'hôte reste inaccessible aux groupes de travails et utilisateurs Active Directory. Vous pouvez utiliser des profils d'hôte afin de configurer un rôle requis pour un utilisateur ou groupes et appliquer le changement à un ou plusieurs hôtes.

Prérequis

Vous devez posséder un profil d'hôte existant. Reportez-vous à « Création d'un profil d'hôte », page 238.

Vérifiez que les hôtes auxquels vous appliquez un profil sont en mode maintenance.

Procédure

1 À l'aide du vSphere Client, sélectionnez **[Afficher]** > **[Gestion]** > **[Profils d'hôte]** .

2 Cliquez avec le bouton droit sur un profil d'hôte existant et sélectionnez **[Modifier le profil]** .

3 Développez l'arborescence de profil, puis **[Configuration de la sécurité]** .

4 Faites un clic avec le bouton droit sur le dossier **[Règles d'autorisation]** , puis sélectionnez **[Ajouter profil]** .

5 Déroulez le menu **[Règles d'autorisation]** et sélectionnez **[Autorisation]** .

6 Sur l'onglet **[Détails configuration]** dans le volet droit, cliquez sur le menu déroulant **[Configurer une autorisation]** et sélectionnez **[Demander une règle d'autorisation]** .

7 Entrez le nom d'un utilisateur ou groupes.

Utilisez le format **`DOMAIN\name`**, où **`DOMAIN`** représente le nom de domaine Active Directory et **`name`** le nom de groupes ou d'utilisateur.

8 (Facultatif) Si vous avez saisi le nom d'un groupes (pas d'un utilisateur unique), cochez la case **[Le nom se réfère à un groupes d'utilisateurs]** .

9 Saisissez le nom du rôle assigné à l'utilisateur ou groupes (généralement **`Admin`**).

Le nom de rôle est sensible à la casse. Si c'est un rôle système, vous devez utiliser le nom de rôle non localisé. Par exemple, pour le rôle Administrateur, saisissez **`Admin`**. Pour le rôle Lecture seule, saisissez **`ReadOnly`**.

10 Cochez la case **[Autorisation de propagation]** , puis cliquez sur **[OK]** .

Suivant

1 Reliez le profil aux hôtes comme indiqué dans « Attacher des entités à partir de l'hôte », page 242.

2 Appliquez le profil aux hôtes comme indiqué dans « Appliquer un profil à partir de l'hôte », page 243.

Chiffrement et certificats de sécurité pour ESX

ESX prend en charge SSL v3 et TLS v1, généralement désignés ici par SSL. 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 de console de service est configuré sur sécurité moyenne ou élevée.

Le contrôle de certificat de l'hôte est activé par défaut et les certificats SSL sont utilisés pour chiffrer le trafic réseau. Néanmoins, ESX utilise des certificats générés automatiquement, créés lors du processus d'installation et stockés sur l'hôte. 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.

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.

L'emplacement par défaut de votre certificat est `/etc/vmware/ssl/` sur l'hôte ESX. Le certificat est composé de deux fichiers : le certificat lui-même (`rui.crt`) et le fichier de clé privée (`rui.key`).

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 un système vCenter Server au moyen de 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 hôte pour ESX, exécutez la commande suivante.

   ```
   openssl x509 –in /etc/vmware/ssl/rui.crt –fingerprint –sha1 –noout
   ```

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 l'hôte ESX

L'hôte ESX génère des certificats la première fois que le système démarre. Dans certaines circonstances, vous devrez peut-être forcer l'hôte à générer de nouveaux certificats. En règle générale, vous générez de nouveaux certificats uniquement si vous changez le nom de l'hôte ou supprimez accidentellement le certificat.

À chaque fois que vous redémarrez le processus `vmware-hostd`, le script `mgmt-vmware` recherche des fichiers de certificats existants (`rui.crt` et `rui.key`). S'il ne les trouve pas, il génère de nouveaux fichiers de certificat.

Procédure

1 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 par accident, vous n'avez pas besoin de les renommer.

2 Pour redémarrer le processus `vmware-hostd`, exécutez la commande suivante :

```
service mgmt-vmware restart
```

3 Confirmez que l'hôte ESX a bien généré de nouveaux certificats en utilisant la commande suivante et en comparant la date et l'heure des nouveaux fichiers de certificats avec celles de orig.rui.crt et orig.rui.key.

```
ls -la
```

Remplacer un certificat par défaut par un certificat signé par une autorité de certification

L'hôte ESX 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.

Procédure

1 Ouvrez une session sur la console de service et procurez-vous des privilèges racines.

2 Dans l'inventaire `/etc/vmware/ssl`, renommez 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 Renommez le nouveau certificat et la clé dans `rui.crt` et `rui.key`.

5 Redémarrez le processus `vmware-hostd` afin que les certificats soient effectifs.

```
service mgmt-vmware restart
```

Configurer les délais d'attente SSL

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

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'ESX.
- Le paramètre Délai d'expiration de négociation s'applique aux connexions qui ont complété le processus de négociation SSL avec le port 443 d'ESX.

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 Ouvrez une session sur la console de service et procurez-vous des privilèges racines.

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 Saisissez la commande suivante pour redémarrer le processus `vmware-hostd` :

```
service mgmt-vmware restart
```

Exemple 13-2. 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 d'ESX

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

Remarque Redémarrez le processus `vmware-hostd` après avoir modifié les répertoires hôtes ou les mécanismes d'authentification en entrant la commande `service mgmt-vmware restart`.

- Ne configurez pas de certificats à l'aide d'expressions relatives au mot de passe. ESX 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 ESX 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 ESX 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 Access et de vSphere Web services SDK. Pour configurer ces connexions afin qu'elles ne chiffrent pas les transmissions, désactivez SSL pour votre connexion vSphere Web Access ou 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 ESX (par exemple, le serveur Web interne qui héberge vSphere Web Access), la plupart des services ESX internes sont uniquement accessibles via le port 443 (port utilisé pour la transmission HTTPS). Le port 443 agit comme proxy inversé pour ESX. Vous pouvez consulter la liste de services sur ESX via une page d'accueil HTTP, mais vous ne pouvez pas directement accéder à ces services 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 ESX dans un environnement parfaitement fiable.
- Lorsque vous mettez vCenter Server et vSphere Web Access à niveau, le certificat est conservé. Si vous retirez vCenter Server et vSphere Web Access, l'inventaire du certificat n'est pas retiré de la console de service.

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. Ouvrez une session sur la console de service et procurez-vous des privilèges racines.
2. Passez au répertoire `/etc/vmware/hostd/`.

3 Utilisez un éditeur de texte pour ouvrir le fichier `proxy.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 ESX 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 ESX utilise ces fichiers.

6 Enregistrez les modifications et fermez le fichier.

7 Saisissez la commande suivante pour redémarrer le processus `vmware-hostd` :

```
service mgmt-vmware 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 Ouvrez une session sur la console de service et procurez-vous des privilèges racines.

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.

- *e id* est un numéro d'ID pour la balise de serveur ID XML. Les numéros d'ID doivent être uniques dans la zone HTTP.
- *_type* est le nom du service que vous transférez.
- *accessmode* représente les 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.
- *port* est le numéro de port attribué au service. Vous pouvez assigner un numéro de port différent au service.
- *serverNamespace* est l'espace de nom du serveur qui fournit ce service, par exemple `/sdk` ou `/mob`.

5 Enregistrez les modifications et fermez le fichier.

6 Saisissez la commande suivante pour redémarrer le processus `vmware-hostd` :

```
service mgmt-vmware restart
```

Exemple 13-3. Configurer vSphere Web Access pour communiquer à travers un port non sécurisé

vSphere Web Access communique normalement avec un hôte ESX via un port sécurisé (HTTPS, 443). Si vous vous trouvez dans un environnement totalement approuvé, vous pouvez décider d'autoriser un port non sécurisé (par exemple, HTTP, 80). Pour le faire, modifiez l'attribut `accessMode` pour le serveur Web dans le fichier `proxy.xml`. Dans le résultat suivant, le mode d'accès `httpsWithRedirect` est remplacé par `httpAndHttps`.

```
<_type>vim.ProxyService.LocalServiceSpec</_type>
<accessMode>httpAndHttps</accessMode>
<port>8080</port>
<serverNamespace>/ui</serverNamespace>
```

14 Sécurité de la console de service

VMware émet quelques recommandations de sécurité de base liées à l'utilisation de la console de service, y compris des recommandations d'utilisation de certaines fonctions de sécurité intégrées de la console du service. La console de service est une interface de gestion ESX : sa sécurité est donc vitale. Pour protéger la console de service contre les intrusions et autorisations illégales, VMware impose des contraintes au niveau de plusieurs paramètres et activités de la console de service.

Ce chapitre aborde les rubriques suivantes :

Recommandations générales de sécurité

Pour protéger la console de service contre les intrusions et autorisations illégales, VMware impose des contraintes au niveau de plusieurs paramètres et activités de la console de service. 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 ESX.

Tenez compte des recommandations suivantes lorsque vous évaluez la sécurité de la console de service et lors de l'administration de celle-ci.

- Limitez l'accès utilisateur.

  Pour augmenter la sécurité, limitez l'accès des utilisateurs à la console de service, et mettez en oeuvre des règles de sécurité d'accès (définissez par exemple des limitations de mots de passe en termes de longueur de caractères, de limite de durée de vie et utilisez un mot de passe GRUB pour le démarrage de l'hôte).

  La console de service possède un accès à certaines parties d'ESX. Par conséquent, vous ne devez octroyer une autorisation d'accès qu'à certains utilisateurs de confiance. Par défaut, l'accès racine est limité (non autorisation de connexion SSH en tant qu'utilisateur racine). Il est recommandé de conserver ce paramétrage par défaut. Exigez que les administrateurs ESX se connectent en tant qu'utilisateurs simples et utilisez la commande `sudo` pour l'exécution de certaines tâches spécifiques nécessitant des privilèges racine.

Par ailleurs, dans la mesure du possible, veillez à exécuter sur la console de service un nombre limité de processus. Idéalement, vous ne devriez exécuter que les processus, services et agents essentiels (tels que les anti-virus, les sauvegardes de machine virtuelle, etc.).

- Utilisez vSphere Client pour gérer les hôtes ESX.

  Utilisez dès que vous le pouvez vSphere Client, vSphere Web Access, ou encore un outil de gestion de réseau tiers pour l'administration de vos hôtes ESX (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 la console de service, 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.

- Vous ne devez utiliser que des sources VMware pour mettre à niveau les composants ESX exécutés sur la console de service.

  Celle-ci utilise un grand nombre de produits tiers (comme par exemple le service Web Tomcat) pour les tâches de gestion à exécuter. WMware 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 la console de service. Visitez régulièrement les sites Web de fournisseurs tiers, ainsi que la base de connaissances VMware pour connaître les alertes de sécurité correspondantes.

Ouverture de session sur la console de service

Les activités de configuration d'ESX s'effectuent via vSphere Client, mais la configuration de certaines fonctions de sécurité s'effectue via l'interface de ligne de commande de la console de service. Pour pouvoir l'utiliser, vous devez ouvrir une session sur l'hôte.

Procédure

1 Ouvrez une session sur l'hôte ESX à l'aide de 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 ESX.

   Si vous effectuez des activités qui nécessitent des privilèges racine, ouvrez une session sur la console de service en tant qu'utilisateur reconnu et procurez-vous des privilèges root via l'exécution de la commande `sudo`, qui présente un niveau de sécurité supérieur à celui de la commande `su`.

Suivant

Outre les commandes propres à ESX, vous pouvez utiliser l'interface de ligne de commande de la console de service pour exécuter un grand nombre d'autres commandes Linux et UNIX. Pour plus d'informations sur les commandes de la console de service, utilisez la commande `man` *`command_name`* pour vérifier les pages Man.

Configuration du pare-feu de la console de service

ESX contient un pare-feu situé entre la console de service et le réseau. Pour garantir l'intégrité de la console de service, VMware a diminué le nombre de ports de pare-feu ouverts par défaut.

Au moment de l'installation, le pare-feu de la console de service est configuré de façon à bloquer tout le trafic entrant et sortant, à l'exception des ports 22, 123, 427, 443, 902, 5989 et 5988, qui sont utilisés pour les communications de base avec ESX. Ce paramétrage applique un niveau de sécurité élevé à l'hôte.

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).

Dans les environnements sécurisés, vous pouvez affecter un niveau de sécurité moins élevé. Dans ce cas, vous pouvez affecter le niveau de sécurité moyen ou faible au pare-feu.

Niveau de sécurité moyen	Tout le trafic entrant est bloqué, sauf sur les ports par défaut et sur ceux qui ont été spécifiés comme étant ouverts. Le trafic sortant n'est pas bloqué.
Niveau de sécurité faible	Aucun bloc ne se trouve dans le trafic entrant ou sortant. Ce paramétrage revient à supprimer le pare-feu.

Les ports ouverts par défaut étant limités de façon stricte, vous devrez peut-être ouvrir d'autres ports après l'installation. Pour obtenir la liste des ports fréquemment utilisés que vous pouvez ouvrir, reportez-vous à« Ports TCP et UDP pour l'accès de gestion », page 171.

Lorsque vous ajoutez les services et les agents de gestion requis pour le bon fonctionnement d'ESX, vous ouvrez d'autres ports sur le pare-feu de la console de service. Pour ajouter des services et des agents de gestion, utilisez vCenter Server, conformément à la description figurant dans« Configuration des ports pare-feu pour les services pris en charge et les agents de gestion », page 168.

Outre les ports que vous ouvrez pour ces services et ces agents, vous pouvez ouvrir d'autres ports au moment de la configuration de certains périphériques, services ou agents (périphériques de stockage, agents de sauvegarde ou agents de gestion, par exemple). Si vous utilisez Veritas NetBackup™ 4.5 en tant qu'agent de sauvegarde par exemple, vous devez ouvrir les ports 13720, 13724, 13782 et 13783, car ils sont utilisés par NetBackup pour les transactions client, les sauvegardes de base de données, les sauvegardes/restaurations utilisateur, notamment. Pour déterminer les ports à ouvrir, consultez les spécifications du fournisseur du périphérique, du service ou de l'agent correspondant.

Remarque Ne modifiez pas les règles par défaut de pare-feu pour la console de service en utilisant une autre commande ou un autre utilitaire que `esxcfg-firewall`. Si vous modifiez les valeurs par défaut via l'exécution d'une commande Linux, vos modifications seront ignorées et écrasées par les valeurs par défaut spécifiées pour ce service par la commande `esxcfg-firewall`.

Détermination du niveau de sécurité du pare-feu de la console de service

La modification du niveau de sécurité de la console de service est un processus qui s'exécute en deux étapes : détermination du niveau de sécurité du pare-feu de la console de service et réinitialisation du paramètre de pare-feu de la console de service. Pour éviter tout changement inutile, vérifiez ce paramètre avant de le modifier.

Procédure

1 Ouvrez une session sur la console de service et procurez-vous des privilèges racines.

2 Utilisez les deux commandes suivantes pour déterminer si le trafic entrant et sortant est bloqué ou autorisé.

```
esxcfg-firewall -q incoming
esxcfg-firewall -q outgoing
```

Interprétez les résultats selon les indications du tableau Tableau 14-1.

Tableau 14-1. Niveaux de sécurité du pare-feu de la console de service

Réponse de la ligne de commande	Niveau de sécurité
`Ports entrants bloqués par défaut.` `Ports sortants bloqués par défaut.`	Elevé
`Ports entrants bloqués par défaut.` `Ports sortants non bloqués par défaut.`	Moyen
`Ports entrants non bloqués par défaut.` `Ports sortants non bloqués par défaut.`	Faible

Définition du niveau de sécurité du pare-feu de la console de service

Une fois que vous avez déterminé le niveau de sécurité applicable au pare-feu de la console de service, vous pouvez définir le niveau de sécurité correspondant. Chaque fois que vous diminuez le niveau de sécurité ou que vous ouvrez des ports supplémentaires, vous augmentez le risque d'intrustion sur le réseau. Vous devez donc trouver un point d'équilibre en fonction du niveau de contrôle que vous souhaitez appliquer à la sécurité du réseau.

Procédure

1 Ouvrez une session sur la console de service et procurez-vous des privilèges racines.

2 Exécutez l'une des commandes suivantes pour définir le niveau de sécurité applicable au pare-feu de la console de service.

- Pour définir un niveau de sécurité moyen, utilisez :

  ```
  esxcfg-firewall --allowOutgoing --blockIncoming
  ```

- Pour définir un niveau de sécurité faible, utilisez :

  ```
  esxcfg-firewall --allowIncoming --allowOutgoing
  ```

AVERTISSEMENT L'utilisation de cette commande désactive totalement la protection du pare-feu.

- Pour rétablir le niveau de sécurité élevé, utilisez :

  ```
  esxcfg-firewall --blockIncoming --blockOutgoing
  ```

3 Pour redémarrer le processus `vmware-hostd`, exécutez la commande suivante :

```
service mgmt-vmware restart
```

La modification du niveau de sécurité du pare-feu de la console de service n'affecte pas les connexions existantes. Par exemple, si le niveau de sécurité du pare-feu est faible et qu'une sauvegarde est exécutée sur un port que vous n'avez pas ouvert explicitement, l'augmentation du niveau de sécurité ne met pas fin à la sauvegarde. La sauvegarde est exécutée jusqu'à son terme, puis la connexion est fermée et aucune autre connexion n'est acceptée pour ce port.

Ouverture d'un port sur le pare-feu de la console de service

Vous pouvez ouvrir des ports sur le pare-feu de la console de service lorsque vous installez des périphériques, des services et des agents tiers. Avant d'ouvrir des ports pour le composant installé, consultez les spécifications du fournisseur afin d'identifier les ports requis.

Prérequis

Vous ne devez utiliser cette procédure que pour ouvrir des ports de services ou d'agents que vous ne pouvez pas configurer via vSphere Client.

AVERTISSEMENT VMware prend en charge l'ouverture et la fermeture de ports de pare-feu uniquement via vSphere Client ou via la commande `esxcfg-firewall`. L'utilisation de toute autre méthode ou d'un script pour l'ouverture de ports de pare-feu risque de déclencher un comportement inattendu.

Procédure

1 Ouvrez une session sur la console de service et procurez-vous des privilèges racines.

2 Pour ouvrir le port, exécutez la commande suivante :

```
esxcfg-firewall --openPort port_number,tcp|udp,in|out,port_name
```

- *port_number* correspond au numéro de port spécifié par le fournisseur.
- Utilisez `tcp` pour le trafic TCP ou `udp` pour le trafic UDP.
- Utilisez `in` pour ouvrir le port pour le trafic entrant ou `out` pour l'ouvrir pour le trafic sortant.
- *port_name* correspond au nom descriptif qui permet d'identifier le service ou l'agent utilisant le port. L'utilisation d'un nom unique n'est pas obligatoire.

Par exemple :

```
esxcfg-firewall --openPort 6380,tcp,in,Navisphere
```

3 Pour redémarrer le processus `vmware-hostd`, exécutez la commande suivante :

```
service mgmt-vmware restart
```

Fermeture d'un port sur le pare-feu de la console de service

Vous pouvez fermer certains ports sur le pare-feu de la console de service. Si vous fermez un port, les sessions actives du service associé au port ne sont pas obligatoirement déconnectées au moment de la fermeture du port. Par exemple, si vous exécutez une sauvegarde et que vous fermez le port de l'agent de sauvegarde, la sauvegarde se poursuit jusqu'à la fin et l'agent libère la connexion.

Vous pouvez utiliser l'option `-closePort` pour fermer uniquement les ports que vous avez ouverts à l'aide de l'option `-openPort`. Si vous avez utilisé une autre méthode pour ouvrir le port, utilisez une méthode équivalente pour le fermer. Par exemple, vous ne pouvez fermer le port SSH (22) que via la désactivation de la connexion entrante du serveur SSH et de la connexion sortante du client SSH dans vSphere Client.

Prérequis

Vous ne devez utiliser cette procédure que pour fermer les ports de services ou d'agents que vous ne pouvez pas configurer via vSphere Client.

AVERTISSEMENT VMware prend en charge l'ouverture et la fermeture de ports de pare-feu uniquement via vSphere Client ou via la commande `esxcfg-firewall`. L'utilisation de toute autre méthode ou d'un script pour l'ouverture ou la fermeture de ports de pare-feu risque de déclencher un comportement inattendu.

Procédure

1 Ouvrez une session sur la console de service et procurez-vous des privilèges racines.

2 Pour fermer le port, exécutez la commande suivante :

```
esxcfg-firewall --closePort port_number,tcp|udp,in|out,port_name
```

L'argument *port_name* est facultatif.

Par exemple :

```
esxcfg-firewall --closePort 6380,tcp,in
```

3 Pour redémarrer le processus `vmware-hostd`, exécutez la commande suivante :

```
service mgmt-vmware restart
```

Dépannage en cas d'écrasement des valeurs de pare-feu

En cas de modification des règles de pare-feu après des opérations de trafic HA WMware, migration, clonage, application de exécution du correctif ou opération vMotion, vous devez configurer les valeurs par défaut de `esxcfg-firewall`

La modification des règles par défaut de pare-feu pour la console de service utilisant une autre commande ou un autre utilitaire que `esxcfg-firewall` n'est pas prise en charge. Si vous modifiez les règles par défaut et que vous tentez ensuite d'accéder à la console de service à l'aide d'un outil ou d'un utilitaire, le pare-feu risque de reprendre sa configuration par défaut une fois les actions exécutées. Par exemple, la configuration du trafic HA sur un hôte risque d'entraîner le rétablissement de la configuration par défaut du pare-feu (spécifiée par `esxcfg-firewall`) si vous avez modifié les règles via l'utilisation d'une autre commande que `esxcfg-firewall`.

Dans la plupart des cas, il est inutile de modifier les règles de pare-feu par défaut pour la console de service. Si vous modifiez les valeurs par défaut via l'exécution d'une commande Linux, vos modifications seront ignorées et écrasées par les valeurs par défaut spécifiées pour ce service par la commande `esxcfg-firewall`. Si vous souhaitez modifier les valeurs par défaut d'un service pris en charge, ou encore celles d'un autre type de service, vous pouvez modifier ou ajouter les règles correspondantes dans `/etc/vmware/firewall/chains/default.xml`.

Procédure

1 Ouvrez une session sur la console de service avec des privilèges d'administrateur.

2 Modifiez le fichier `/etc/vmware/firewall/chains/default.xml` afin qu'il reflète vos règles de sécurité.

3 Redémarrez le pare-feu de la console de service via l'utilisation de la commande `service firewall restart`.

4 Pour vérifier que les services spécifiés sont correctement activés ou désactivés, utilisez la commande `esxcfg-firewall-e|d SERVICE`.

Exemple 14-1. Modification de la chaîne INPUT

Vous pouvez modifier les valeurs par défaut du pare-feu pour chaque type de service, en fonction de vos propres règles de sécurité. Par exemple, les règles suivantes du fichier `/etc/vmware/firewall/chains/default.xml` déterminent les règles de pare-feu pour la chaîne `INPUT` :

```
<ConfigRoot>
  <chain name="INPUT">
    <rule>-p tcp --dport 80 -j ACCEPT</rule>
    <rule>-p tcp --dport 110 -j ACCEPT</rule>
    <rule>-p tcp --dport 25 -j ACCEPT</rule>
  </chain>...
</ConfigRoot>
```

Limitations liées aux mots de passe

La facilité avec laquelle un pirate parvient à se connecter à un hôte ESX dépend de sa capacité à trouver une combinaison autorisée de nom d'utilisateur et mot de passe. Vous pouvez définir des limitations pour les mots de passe, afin d'éviter que les pirates n'obtiennent les mots de passe des utilisateurs.

Un utilisateur malveillant peut obtenir un mot de passe de différentes façons. Par exemple, un pirate peut détecter un trafic réseau peu sécurisé (transmissions Telnet ou FTP, par exemple) et faire une tentative de connexion. Il existe une autre méthode : obtenir le mot de passe via l'exécution d'un générateur de mots de passe, qui essaie chaque combinaison de caractères jusqu'à une longueur définie, ou qui utilise des mots réels et des mutations simples de mots réels.

La mise en oeuvre de limitations qui régissent la longueur, les jeux de caractères et la durée des mots de passe peut rendre plus difficiles les attaques lancées via un générateur de mots de passe. Plus un mot de passe est long et complexe, plus le pirate a du mal à le trouver. Plus la fréquence de changement de mot de passe par les utilisateurs est élevée, plus il est difficile de trouver un mot de passe pouvant être utilisé plusieurs fois.

Remarque Tenez toujours compte du facteur humain lorsque vous déterminez les limitations de mot de passe à mettre en oeuvre. En effet, si vos mots de passe sont trop difficiles à mémoriser ou entraînent de fréquentes modifications, vos utilisateurs auront tendance à les noter, ce qui ôte tout le bénéfice de la méthode.

Pour protéger votre base de données de mots de passe contre les utilisations malveillantes, un ombrage de mot de passe est activé, qui permet de masquer les hachages de mots de passe. ESX utilise également les mots de passe MD5, qui offrent une sécurité renforcée et permettent de définir des exigences de longueur (d'une longueur minimale à plus de huit caractères).

Durée de vie des mots de passe

Vous pouvez imposer des limitations de durée de vie des mots de passe pour vous assurer que les mots de passe des utilisateurs ne restent pas actifs pendant de trop longues périodes.

ESX impose les limitations de durée de vie des mots de passe suivantes pour les connexions utilisateur par défaut :

Nombre de jours maximum	Nombre de jours pendant lequel un utilisateur peut conserver un mot de passe. Par défaut, les mots de passe sont définis avec un délai d'expiration illimité.
Nombre de jours minimum	Nombre de jours minimum à respecter entre deux modifications de mot de passe. La valeur par défaut est 0, ce qui signifie que les utilisateurs peuvent modifier à tout moment leurs mots de passe.
Jour d'avertissement	Nombre de jours de préavis pour l'envoi d'un rappel signalant l'expiration du mot de passe. La valeur par défaut est sept jours. Les avertissements ne s'affichent que lors des connexions directes à la console de service ou de l'utilisation de SSH.

Vous pouvez affecter à ces paramètres une valeur plus élevée ou plus faible. Vous pouvez également remplacer les valeurs de durée de vie de mots de passe pour un utilisateur ou un groupes spécifique.

Modification des limitations de durée de vie des mots de passe par défaut d'un hôte

Vous pouvez imposer l'application aux hôtes de limitations de durée de vie de mots de passe plus strictes ou moins strictes que celles fournies par défaut.

Procédure

1 Ouvrez une session sur la console de service et procurez-vous des privilèges racines.

2 Pour modifier le nombre de jours maximum pendant lequel un utilisateur peut conserver un mot de passe, utilisez la commande suivante :

```
esxcfg-auth --passmaxdays=number_of_days
```

3 Pour modifier le nombre de jours minimum à respecter entre deux modifications de mot de passe, utilisez la commande suivante :

```
esxcfg-auth --passmindays=number_of_days
```

4 Pour modifier la durée d'avertissement avant changement de mot de passe, utilisez la commande suivante :

```
esxcfg-auth --passwarnage=number_of_days
```

Modification des limitations de durée de vie par défaut des mots de passe utilisateur

Vous pouvez remplacer les limitations par défaut de durée de vie des mots de passe pour des utilisateurs ou des groupes spécifiques.

Procédure

1 Ouvrez une session sur la console de service et procurez-vous des privilèges racines.

2 Pour modifier le nombre de jours maximum, utilisez la commande suivante :

```
chage –M number_of_days username
```

3 Pour modifier le jour de l'avertissement, utilisez la commande suivante :

```
chage –W number_of_days username
```

4 Pour modifier le nombre de jours minimum, utilisez la commande suivante :

```
chage –m number_of_days username
```

Niveau de sécurité et complexité des mots de passe

Par défaut, ESX 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, ESX 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 :

- *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. ESX exige trois mots par 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 ESX. Vous ne pouvez pas spécifier ces paramètres supplémentaires dans `esxcfg–auth`.

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 Ouvrez une session sur la console de service et procurez-vous des privilèges racines.

2 Entrez la commande suivante :

```
esxcfg–auth ––usepamqc=N0N1N2N3N4match
```

Exemple 14-2. Command'ESXcfg-auth --usepamqc

Par exemple, vous pouvez utiliser la commande suivante :

```
esxcfg–auth ––usepamqc=disabled 18 –1 12 8
```

Une fois ce paramètre activé, un utilisateur créant un mot de passe ne peut pas définir de mots de passe contenant une seule classe de caractères. Il doit utiliser au minimum 18 caractères par mot de passe à deux classes de caractères, 12 caractères pour les mots de passe à trois classes de caractères et 8 caractères pour les mots de passe à quatre classes de caractères. Les tentatives de création de phrases de passe sont ignorées.

Configuration d'une règle de réutilisation des mots de passe

Vous pouvez définir le nombre d'anciens mots de passe stockés pour chaque utilisateur.

Procédure

1 Ouvrez une session sur la console de service et procurez-vous des privilèges racines.

2 Accédez au répertoire `/etc/pam.d/`.

3 Utilisez un éditeur de texte pour ouvrir le fichier `system–auth–generic`.

4 Recherchez la ligne commençant par `password sufficient /lib/security/$ISA/pam_unix.so`.

5 Ajoutez le paramètre suivant à la fin de la ligne, où `X` correspond au nombre d'anciens mots de passe à stocker pour chaque utilisateur.

```
remember=X
```

Utilisez un espace entre les différents paramètres.

6 Enregistrez les modifications et fermez le fichier.

7 Accédez au répertoire `/etc/security/` et utilisez la commande suivante pour créer un fichier à longueur zéro (0) utilisant `opasswd` comme nom de fichier.

```
touch opasswd
```

8 Entrez les commandes suivantes :

```
chmod 0600 opasswd
chown root:root /etc/security/opasswd
```

Utilisation du plug-in d'authentification pam_cracklib.so

Le plug-in d'authentification par défaut d'ESX est `pam_passwdqc.so`, qui permet d'appliquer des règles strictes aux mots de passe de la plupart des environnements. Si ce plug-in n'est pas adapté à votre environnement, vous pouvez utiliser à la place le plug-in `pam_cracklib.so`.

Le plug-in `pam_cracklib.so` vérifie toutes les tentatives de modification de mot de passe pour s'assurer que les critères de sécurité sont respectés.

- Le nouveau mot de passe ne doit pas être un palindrome. Un palindrome est un terme dont les lettres peuvent être lues dans les deux sens, comme radar ou kayak.
- Il ne doit pas non plus être l'inverse de l'ancien mot de passe.
- Le nouveau mot de passe ne doit pas être une rotation. Une rotation est une version de l'ancien mot de passe dans laquelle un ou plusieurs caractères ont subi une rotation vers l'avant ou l'arrière du mot de passe.
- Il doit se démarquer de l'ancien mot de passe via d'autres éléments que le seul changement de casse.
- Il doit comporter plusieurs caractères différents de ceux de l'ancien mot de passe.
- Il ne doit pas avoir été déjà utilisé. Le plug-in `pam_cracklib.so` n'applique ces critères que si vous avez configuré une règle de réutilisation des mots de passe.

  Par défaut, ESX n'impose pas de règle de réutilisation de mot de passe ; par conséquent, le plug-in `pam_cracklib.so` ne rejette jamais une tentative de modification de mot de passe en fonction de ce critère. Toutefois, vous pouvez configurer une règle de réutilisation afin de garantir que vos utilisateurs n'utilisent pas en alternance quelques mots de passe uniquement.

  Si vous configurez une règle de réutilisation, les anciens mots de passe sont stockés dans un fichier auquel le plug-in `pam_cracklib.so` fait référence lors de chaque tentative de modification de mot de passe. Les règles de réutilisation déterminent le nombre d'anciens mots de passe conservés par ESX. Lorsqu'un utilisateur crée un nombre suffisant de mots de passe pour atteindre la valeur spécifiée dans la règle de réutilisation, les anciens mots de passe sont supprimés du fichier, par ordre d'ancienneté.
- Le nouveau mot de passe doit être assez long et complexe pour ce que requiert le plug-in. Configurez ces paramètres en changeant les paramètres de complexité `pam_cracklib.so` avec la commande `esxcfg-auth`, qui permet de définir le nombre d'essais, la longueur minimale du mot de passe et plusieurs options de caractères.

Pour définir la complexité des mots de passe à l'aide du plug-in `pam_cracklib.so`, vous pouvez affecter des valeurs aux paramètres de caractères autorisés, pour chacune des classes de caractères suivantes :

- *lc_credit* représente les lettres minuscules
- *uc_credit* représente les lettres majuscules
- *d_credit* représente les nombres
- *oc_credit* représente les caractères spéciaux (trait de soulignement ou tiret, par exemple).

Les caractères autorisés viennent s'ajouter au score de complexité d'un mot de passe. Un mot de passe utilisateur doit correspondre au score minimum ou le dépasser ; vous pouvez définir cette valeur à l'aide du paramètre *minimum_length*.

Remarque Le plug-in `pam_cracklib.so` n'accepte pas les mots de passe composés de moins de six caractères, quelles que soient les valeurs utilisées et la valeur affectée à *minimum_length*. En d'autres termes, si la valeur affectée à *minimum_length* est 5, les utilisateurs doivent malgré tout entrer au moins six caractères.

Pour déterminer si un mot de passe est acceptable, le plug-in `pam_cracklib.so` utilise plusieurs règles de calcul de score de mot de passe.

- Chaque caractère du mot de passe (quel que soit son type) compte pour un dans le paramètre *minimum_length*.
- Les valeurs autres que zéro affectent la complexité des mots de passe, selon que des valeurs négatives ou positives sont utilisées.
  - Pour les valeurs positives, ajoutez un caractère autorisé à la classe de caractères, jusqu'à atteindre le nombre maximum spécifié par ce paramètre.

    Par exemple, si la valeur de *lc_credit* est égale à 1, ajoutez au mot de passe un caractère autorisé dans la classe des lettres minuscules. Dans ce cas, 1 correspond au nombre maximum autorisé pour les lettres minuscules, quel que soit le nombre utilisé.
  - Pour les valeurs négatives, n'ajoutez pas de caractère autorisé à la classe correspondante, mais exigez que cette classe soit utilisée un nombre minimum de fois. Ce nombre minimum est spécifié par le paramètre de caractères autorisés.

    Par exemple, si la valeur de *uc_credit* est égale à -1, les mots de passe doivent contenir au minimum un caractère en majuscules. Dans ce cas, aucun caractère autorisé supplémentaire n'est accordé pour les lettres en majuscules, quel que soit le nombre utilisé.
- Les classes de caractères comportant une valeur égale à zéro sont comptabilisées dans la longueur totale du mot de passe, mais elles ne font pas l'objet de caractères autorisés supplémentaires et ne sont pas obligatoires. Vous pouvez définir une valeur égale à zéro pour toutes les classes de caractères, afin d'imposer une longueur de mot de passe, sans tenir compte de la complexité.

  Par exemple, les mots de passe **`xyzpqets`** et **`Xyzpq3#s`** affichent tous deux un score de huit.

Basculement vers le plug-in pam_cracklib.so

Par rapport au plug-in `pam_passwdqc.so`, le plug-in `pam_cracklib.so` offre moins d'options d'ajustement du niveau de sécurité des mots de passe, et n'exécute pas les tests de niveau de sécurité des mots de passe pour tous les utilisateurs. Toutefois, si le plug-in `pam_cracklib.so` est plus adapté à votre environnement, vous pouvez effectuer un basculement entre le plug-in par défaut `pam_passwdqc.so` vers le plug-in `pam_cracklib.so`.

Remarque Le plug-in `pam_cracklib.so` utilisé dans Linux offre davantage de paramètres que ceux pris en charge pour ESX. Vous ne pouvez pas spécifier ces paramètres supplémentaires dans `esxcfg-auth`. Pour plus d'informations sur ce plug-in, consultez la documentation Linux.

Procédure

1 Ouvrez une session sur la console de service et procurez-vous des privilèges racines.

2 Exécutez la commande suivante.

```
esxcfg-auth --usecrack=retriesminimum_lengthlc_credituc_creditd_creditoc_credit
```

- *retries*: nombre de tentatives autorisées avant blocage.
- *minimum_length*: score (ou longueur efficace) de mot de passe minimum après application des différentes valeurs.

  Remarque Le plug-in `pam_cracklib.so` n'accepte pas les mots de passe composés de moins de six caractères, quelles que soient les valeurs utilisées et la valeur affectée à *minimum_length*. En d'autres termes, si la valeur affectée à *minimum_length* est 5, les utilisateurs doivent malgré tout entrer au moins six caractères.

- *lc_credit*: nombre maximum de valeurs autorisées en lettres minuscules.
- *uc_credit*: nombre maximum de valeurs autorisées en lettres majuscules.
- *d_credit*: nombre maximum de valeurs autorisées en chiffres.
- *oc_credit*: nombre maximum de valeurs autorisées pour les caractères spéciaux (traits de soulignement ou tiret, par exemple).

Les exigences du plug-in au niveau du mot de passe sont configurées en fonction des paramètres que vous avez saisis.

Exemple 14-3. Command'ESXcfg-auth --usecrack

```
esxcfg-auth --usecrack=3 9 1 -1 -1 1
```

- Les utilisateurs peuvent effectuer trois tentatives de saisie de mot de passe avant verrouillage.
- Le score du mot de passe doit être égal à neuf.
- Une valeur en lettres minuscules est autorisée au maximum.
- Une lettre majuscule est obligatoire. Aucune autre valeur ne doit être saisie pour ce type de caractère.
- Il doit contenir au moins un chiffre. Aucune autre valeur ne doit être saisie pour ce type de caractère.
- Une valeur en caractères spéciaux est autorisée au maximum.

A l'aide de ces exemples de valeurs, le mot de passe **`xyzpqe#`** serait refusé :

```
(x + y + z + p +q + e + #) + (lc_credit + oc_credit) = 9
```

Le score du mot de passe est égal à neuf, mais il ne contient pas les valeurs requises au niveau de la lettre majuscule et du chiffre.

En revanche, le mot de passe **`Xyzpq3#`** serait accepté :

```
(X + y + z + p +q + 3 + #) + (lc_credit + oc_credit) = 9
```

En effet, son score est également de neuf, mais il inclut les valeurs requises au niveau de la majuscule et du chiffre. La lettre majuscule et le chiffre n'ajoutent pas de point supplémentaire.

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 sécurité, 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, ESX utilise l'un des chiffrements les plus sécurisés du marché : le chiffrement AES 256 bits. Pour les échanges de clés, ESX 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 l'hôte ESX, via la console de service.
- Connexions vSphere Web Access vers l'hôte ESX, via la console de service.

  Remarque L'utilisation du chiffrement vSphere Web Access est déterminé par le navigateur Web que vous utilisez ; cet outil de gestion peut utiliser d'autres méthodes de chiffrement.
- Connexions SDK vers vCenter Server et vers ESX.
- Connexions de la console de service vers des machines virtuelles, via VMkernel.
- Connexions SSH vers l'hôte ESX, via la console de service.

Indicateurs setuid et setgid

Au cours de l'installation d'ESX, plusieurs applications incluant les indicateurs `setuid` et `setgid` sont installées par défaut. Certaines applications contiennent les outils requis pour le bon fonctionnement de l'hôte. D'autres outils sont facultatifs, mais ils facilitent la gestion et le dépannage de l'hôte et du réseau.

setuid Indicateur permettant à une application de modifier temporairement les autorisations de l'utilisateur via l'affectation de l'ID utilisateur du propriétaire du programme à l'utilisateur de l'application.

setgid Indicateur permettant à une application de modifier temporairement les autorisations du groupes via l'affectation de l'ID de groupes du propriétaire du programme au groupes utilisateur de l'application.

Désactivation des applications facultatives

La désactivation d'une application obligatoire entraîne des problèmes au niveau de l'authentification ESX et du fonctionnement des machines virtuelles ; en revanche, vous pouvez mettre hors tension les applications facultatives.

Les applications facultatives sont répertoriées dans Tableau 14-2 et dansTableau 14-3.

Procédure

1 Ouvrez une session sur la console de service et procurez-vous des privilèges racines.

2 Pour mettre hors tension l'application, exécutez l'une des commandes suivantes :

- Pour les applications avec indicateurs `setuid` :

  `chmod a-s` *`path_to_executable_file`*

- Pour les applications avec indicateurs `setgid` :

  `chmod a-g` *`path_to_executable_file`*

Applications setuid par défaut

Par défaut, plusieurs applications incluant l'indicateur `setuid` sont installées.

Tableau 14-2 énumère les applications `setuid` par défaut et indique si l'application est requise ou facultative.

Tableau 14-2. Applications setuid par défaut

Application	Objectif et chemin	Requis ou facultatif
`crontab`	Permet aux utilisateurs d'ajouter des travaux. Chemin : `/usr/bin/crontab`	Optionnel
`pam_timestamp_check`	Prend en charge l'authentification des mots de passe. Chemin : `/sbin/pam_timestamp_check`	requis
`passwd`	Prend en charge l'authentification des mots de passe. Chemin : `/usr/bin/passwd`	requis
`ping`	Envoie des paquets de contrôle à l'interface réseau et les écoute. Cetta application est utile pour le débogage de réseaux. Chemin : `/bin/ping`	Optionnel
`pwdb_chkpwd`	Prend en charge l'authentification des mots de passe. Chemin : `/sbin/pwdb_chkpwd`	requis
`ssh-keysign`	Effectue l'authentification basée sur les hôtes pour SSH. Chemin : `/usr/libexec/openssh/ssh-keysign`	Obligatoire si vous utilisez l'authentification basée sur les hôtes. Sinon, application facultative.
`su`	Permet aux utilisateurs de devenir utilisateurs racine via le changement d'utilisateurs. Chemin : `/bin/su`	requis
`sudo`	Permet aux utilisateurs de devenir utilisateurs racine pour des opérations spécifiques uniquement. Chemin : `/usr/bin/sudo`	Optionnel
`unix_chkpwd`	Prend en charge l'authentification des mots de passe. Chemin : `/sbin/unix_chkpwd`	requis
`vmkload_app`	Exécute les tâches requises pour l'exécution des machines virtuelles. Cette application est installée à deux emplacements : à un emplacement pour les utilisations standard et à un autre emplacement pour le débogage. Chemin pour les utilisations standard : `/usr/lib/vmware/bin/vmkload_app` Chemin pour le débogage : `/usr/lib/vmware/bin-debug/vmkload_app`	Obligatoire aux deux emplacements

Tableau 14-2. Applications setuid par défaut (suite)

Application	Objectif et chemin	Requis ou facultatif
`vmware-authd`	Permet d'authentifier les utilisateurs en vue de l'utilisation de services propres à VMware. Chemin : `/usr/sbin/vmware-authd`	requis
`vmware-vmx`	Exécute les tâches requises pour l'exécution des machines virtuelles. Cette application est installée à deux emplacements : à un emplacement pour les utilisations standard et à un autre emplacement pour le débogage. Chemin pour les utilisations standard : `/usr/lib/vmware/bin/vmware-vmx` Chemin pour le débogage : /usr/lib/vmware/bin-debug/vmware-vmk	Obligatoire aux deux emplacements

Applications setgid par défaut

Par défaut, deux applications incluant l'indicateur `setgid` sont installées.

Tableau 14-3 énumère les applications `setgid` par défaut et indique si l'application est requise ou facultative.

Tableau 14-3. Applications `setgid` par défaut

Application	Objectif et chemin	Requis ou facultatif
`wall`	Alerte tous les terminaux de l'exécution imminente d'une action. Cette application est appelée par la commande `shutdown` et par d'autres commandes. Chemin : `/usr/bin/wall`	optionnel
`lockfile`	Effectue le verrouillage de l'agent de gestion Dell OM. Chemin : `/usr/bin/lockfile`	Obligatoire pour Dell OM, sinon facultative

Sécurité SSH

SSH est un shell de commande Unix et Linux fréquemment utilisé ; il permet d'ouvrir une session à distance sur la console de service et d'exécuter certaines tâches de gestion et de configuration de l'hôte. Il est utilisé pour bénéficier d'ouvertures de sessions et de transferts de données sécurisés, car il offre une protection plus élevée que les autres shells de commande.

Dans cette versions d'ESX, la configuration SSH a été améliorée, dans le but d'offrir un niveau de sécurité renforcé. Cette amélioration inclut principalement les fonctions suivantes :

- Désactivation de la version 1 du protocole SSH – VMware ne prend plus en charge le protocole SSH version 1. 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 interface de communication plus sûre avec la console de service.
- Chiffrement renforcé – Pour les connexions, SSH ne prend désormais en charge que les chiffrements AES 256 bits et 128 bits.
- Limitation des connexions racine – Vous ne pouvez plus vous connecter à distance en tant qu'utilisateur racine. Vous devez vous connecter en tant qu'utilisateur identifiable, et utiliser soit la commande `sudo` pour l'exécution de commandes spécifiques nécessitant des privilèges racines, soit la commande `su` pour devenir utilisateur racine.

REMARQUE La commande `sudo` présente des avantages en termes de sécurité : elle limite les activités racine et permet de vérifier les éventuelles erreurs d'utilisation des autorisations racine, en générant une piste d'audit de ces activités exécutées par l'utilisateur.

Ces paramètres sont destinés à assurer une protection renforcée des données transmises à la console de service via SSH. Si cette configuration est trop rigide, vous pouvez diminuer les valeurs affectées aux paramètres de sécurité.

Modification de la configuration SSH par défaut

Vous pouvez modifier la configuration SSH par défaut.

Procédure

1 Ouvrez une session sur la console de service et procurez-vous des privilèges racines.

2 Accédez au répertoire `/etc/ssh`.

3 Utilisez un éditeur de texte pour exécuter l'une des actions suivantes dans le fichier `sshd_config`.

- Pour autoriser les connexions racine à distance, modifiez le paramètre en spécifiant `yes` sur la ligne suivante :

  ```
  PermitRootLogin no
  ```

- Pour rétablir le protocole SSH par défaut (version 1 et 2), désactivez la ligne suivante :

  ```
  Protocol 2
  ```

- Pour restaurer le chiffrement 3DES et d'autres chiffrements, désactivez la ligne suivante :

  ```
  Ciphers aes256-cbc,aes128-cbc
  ```

- Pour mettre hors tension FTP (SFTP) sur SSH, désactivez la ligne suivante :

  ```
  Subsystem ftp /usr/libexec/openssh/sftp-server
  ```

4 Enregistrez les modifications et fermez le fichier.

5 Exécutez la commande suivante pour redémarrer le service SSHD :

```
service sshd restart
```

Correctifs de sécurité et logiciels d'analyse de vulnérabilité de sécurité

Certains scanners de sécurité tels que Nessus vérifient le numéro de version, mais ne vérifient pas le suffixe du correctif. Par conséquent, ils peuvent générer des rapports indiquant de façon erronée qu'un logiciel n'inclut pas les correctifs de sécurité les plus récents. Dans ce cas, vous pouvez effectuer quelques vérifications.

Ce problème est fréquent et n'est pas propre à VMware. Certains scanners de sécurité peuvent gérer correctement cette situation, mais ils affichent souvent un décalage d'une version, voire plus. Par exemple, la version de Nessus lancée après un correctif Red Hat ne signale pas ces faux positifs dans bien des cas.

Si un correctif de logiciel Linux pris en charge, fourni par VMware en tant que composant de la console de service est lancé sur le marché (service, outil ou protocole notamment), VMware émet une note d'information contenant la liste des composants VIB (vSphere Installation Bundles) à utiliser pour la mise à niveau de ce logiciel sous ESX. Ces correctifs peuvent également être disponibles auprès d'autres sources. Veillez donc à lire les notes d'information VMware et évitez d'utiliser des produits RPM Package Manager tiers.

La politique de VMware en matière de correctifs logiciels consiste à utiliser une version stable. Cette approche diminue les risques de survenue de nouveaux problèmes ou d'instabilité dans le logiciel. Le correctif est ajouté à une version existante du logiciel ; par conséquent, le numéro de version reste le même, mais le numéro du correctif est ajouté sous forme de suffixe.

Voici un exemple illustrant la survenue de ce problème :

1. Vous installez à l'origine ESX avec OpenSSL version 0.9.7a (qui correspond à la version d'origine, sans correctifs).
2. OpenSSL émet un correctif de sécurité correspondant à la version 0.9.7. Cette version est la version 0.9.7x.
3. VMware émet le correctif OpenSSL 0.9.7x pour la version d'origine, met à niveau le numéro du correctif et crée un VIB. La version OpenSSL figurant dans le VIB est la version 0.9.7a-1, ce qui indique que la version d'origine (0.9.7a) contient désormais le correctif 1.
4. Ensuite, vous installez les mises à niveau.
5. Le scanner de sécurité ne remarque pas le suffixe -1 et signale par erreur que la sécurité OpenSSL n'est pas à niveau.

Si votre scanner indique que la sécurité d'un produit n'est pas à niveau, effectuez les vérifications suivantes.

- Recherchez le suffixe du correctif, afin de déterminer si une mise à niveau est requise.
- Lisez la documentation VMware VIB pour plus d'informations sur le contenu du correctif.
- Recherchez le numéro CVE (Common Vulnerabilities and Exposures) dans l'alerte de sécurité du journal de mise à niveau logicielle.

  S'il y figure, cela signifie que le produit spécifié inclut cette vulnérabilité.

Meilleures pratiques en matière de sécurité et scénarios de sécurité 15

Une série de scénarios de déploiement ESX a été élaborée pour permettre une utilisation optimale des fonctions de sécurité au sein de votre propre déploiement. Ces scénarios contiennent également des recommandations de base en matière de sécurité. Elles vous seront utiles lors de la création et de la configuration de machines virtuelles.

Ce chapitre aborde les rubriques suivantes :

Approches de sécurité pour les déploiements ESX classiques

Vous pouvez comparer les approches de sécurité de différents types de déploiements, afin d'optimiser la planification de la sécurité applicable à votre propre déploiement ESX.

La complexité des déploiements ESX est susceptible de varier considérablement en fonction de la taille de votre entreprise, du mode de partage des données et des ressources avec le monde extérieur, du nombre de centres de données, etc. Cependant, les règles d'accès utilisateur, le partage des ressources et le niveau de sécurité se retrouvent dans tous les déploiements suivants.

Déploiement à client unique

Dans un déploiement à client unique, les hôtes ESX appartiennent à une seule entreprise et à un seul centre de données, et sont gérés par ces derniers. Les ressources hôte ne sont pas partagées avec les utilisateurs externes. Un administrateur de site gère les hôtes, qui sont exécutés sur un certain nombre de machines virtuelles.

Le déploiement à client unique n'inclut pas d'administrateurs clients ; l'administrateur de site est le seul responsable de la gestion des différentes machines virtuelles. L'entreprise affecte des administrateurs système, qui ne disposent pas de compte pour l'hôte et ne peuvent donc pas accéder aux outils ESX tels que vCenter Server, ou encore aux shells de ligne de commande de l'hôte. Ces administrateurs système ont accès aux machines virtuelles via la console de la machine virtuelle : ils peuvent donc charger des logiciels et exécuter d'autres tâches de maintenance sur les machines virtuelles.

Le Tableau 15-1 illustre le partage possible des composants utilisés et configurés pour l'hôte.

Tableau 15-1. Partage de composants au sein d'un déploiement à client unique

Fonction	Configuration	Commentaires
La console de service partage-t-elle le même réseau physique que les machines virtuelles ?	Non	Isolez la console de service en la configurant sur son propre réseau physique.
La console de service partage-t-elle le même réseau VLAN que les machines virtuelles ?	Non	Isolez la console de service en la configurant sur son propre réseau VLAN. Aucune machine virtuelle et aucun autre outil système (tel que vMotion) ne doit utiliser ce réseau VLAN.
Les machines virtuelles partagent-elles le même réseau physique ?	Oui	Configurez les machines virtuelles sur le même réseau physique.
Existe-t-il un partage de cartes réseau ?	Partage partiel	Isolez la console de service en la configurant sur son propre commutateur virtuel et sur sa propre carte réseau virtuelle. Aucune machine virtuelle, aucun autre outil système ne doit utiliser ce commutateur ou cette carte. Vous pouvez configurer vos machines virtuelles sur le même commutateur virtuel et sur la même carte réseau.
Existe-t-il un partage VMFS ?	Oui	Tous les fichiers `.vmdk` résident sur la même partition VMFS.
Niveau de sécurité	Élevé	Ouvrez individuellement les ports requis pour les services dont vous avez besoin (FTP, par exemple). Consultez la rubrique « Configuration du pare-feu de la console de service », page 208 pour plus d'informations sur les niveaux de sécurité.
Existe-t-il un engagement excessif de la mémoire des machines virtuelles ?	Oui	Configurez une quantité totale de mémoire des machines virtuelles égale à celle de la mémoire physique.

Le Tableau 15-2 illustre la configuration possible des comptes d'utilisateur pour l'hôte.

Tableau 15-2. Configuration de comptes d'utilisateur au sein d'un déploiement à client unique

Catégorie d'utilisateur	Nombre total de comptes
Administrateurs de site	1
Administrateurs clients	0
Administrateurs système	0
Utilisateurs	0

Le Tableau 15-3 indique le niveau d'accès de chaque utilisateur.

Tableau 15-3. Accès des utilisateurs au sein d'un déploiement à client unique

Niveau d'accès	Administrateur de site	Administrateur système
Accès racine?	Oui	Non
Accès par la console de service via SSH ?	Oui	Non
Accès au Web via vCenter Server et vSphere ?	Oui	Non
Création et modification de machine virtuelle ?	Oui	Non
Accès aux machines virtuelles via la console ?	Oui	Oui

Déploiement limité à clients multiples

Dans les déploiements limités à clients multiples, les hôtes ESX sont situés dans le même centre de données et sont utilisés pour la fourniture d'applications à des clients multiples. L'administrateur du site est chargé de gérer les hôtes ; ceux-ci sont exécutés sur des machines virtuelles dédiées aux clients. Les machines virtuelles rattachées aux différents clients peuvent se trouver sur le même hôte, mais l'administrateur du site limite le partage de ressources afin d'empêcher les interactions non autorisées.

Bien qu'il n'y ait qu'un seul administrateur de site, plusieurs administrateurs clients peuvent gérer les machines virtuelles rattachées à leurs clients. Ce déploiement inclut également des administrateurs système de clients qui ne possèdent pas de compte ESX, mais qui ont accès aux machines virtuelles via la console, et qui peuvent donc charger des logiciels et exécuter d'autres tâches de maintenance sur les machines virtuelles.

Le Tableau 15-4 illustre le partage possible des composants utilisés et configurés pour l'hôte.

Tableau 15-4. Partage de composants au sein d'un déploiement limité à clients multiples

Fonction	Configuration	Commentaires
La console de service partage-t-elle le même réseau physique que les machines virtuelles ?	Non	Isolez la console de service en la configurant sur son propre réseau physique.
La console de service partage-t-elle le même réseau VLAN que les machines virtuelles ?	Non	Isolez la console de service en la configurant sur son propre réseau VLAN. Aucune machine virtuelle et aucun autre outil système (tel que vMotion) ne doit utiliser ce réseau VLAN.
Les machines virtuelles partagent-elles le même réseau physique ?	Partage partiel	Placez les machines virtuelles de chaque client sur un réseau physique différent. Tous les réseaux physiques sont indépendants les uns des autres.
Existe-t-il un partage de cartes réseau ?	Partage partiel	Isolez la console de service en la configurant sur son propre commutateur virtuel et sur sa propre carte réseau virtuelle. Aucune machine virtuelle, aucun autre outil système ne doit utiliser ce commutateur ou cette carte. Vous devez configurer les machines virtuelles pour un client, afin qu'elles partagent toutes le même commutateur virtuel et la même carte réseau. Elles ne partagent pas le commutateur et la carte avec d'autres clients.
Existe-t-il un partage VMFS ?	Non	Chaque client possède sa propre partition VMFS et les fichiers de la machine virtuelle `.vmdk` résident exclusivement sur cette partition. Celle-ci peut s'étendre sur plusieurs LUN.
Niveau de sécurité	Élevé	Permet d'ouvrir les ports de services tels que FTP, en cas de besoin.
Existe-t-il un engagement excessif de la mémoire des machines virtuelles ?	Oui	Configurez une quantité totale de mémoire des machines virtuelles égale à celle de la mémoire physique.

Le Tableau 15-5 illustre la configuration possible des comptes d'utilisateur pour l'hôte ESX.

Tableau 15-5. Configuration de comptes d'utilisateur au sein d'un déploiement limité à clients multiples

Catégorie d'utilisateur	Nombre total de comptes
Administrateurs de site	1
Administrateurs clients	10
Administrateurs système	0
Utilisateurs	0

Le Tableau 15-6 indique le niveau d'accès de chaque utilisateur.

Tableau 15-6. Accès des utilisateurs au sein d'un déploiement limité à clients multiples

Niveau d'accès	Administrateur de site	Administrateur client	Administrateur système
Accès racine?	Oui	Non	Non
Accès par la console de service via SSH ?	Oui	Oui	Non
Accès au Web via vCenter Server et vSphere ?	Oui	Oui	Non
Création et modification de machine virtuelle ?	Oui	Oui	Non
Accès aux machines virtuelles via la console ?	Oui	Oui	Oui

Déploiement ouvert à clients multiples

Dans les déploiements ouverts à clients multiples, les hôtes ESX sont situés dans le même centre de données et sont utilisés pour la fourniture d'applications à des clients multiples. L'administrateur du site est chargé de gérer les hôtes ; ceux-ci sont exécutés sur des machines virtuelles dédiées aux clients. Les machines virtuelles rattachées aux différents clients peuvent résider sur le même hôte, mais les limitations de partage de ressources sont moins nombreuses.

Bien qu'il n'y ait qu'un seul administrateur de site dans le cas d'un déploiement ouvert à clients multiples, plusieurs administrateurs clients peuvent gérer les machines virtuelles rattachées à leurs clients. Ce déploiement inclut également des administrateurs système de clients qui ne possèdent pas de compte ESX, mais qui ont accès aux machines virtuelles via la console, et qui peuvent donc charger des logiciels et exécuter d'autres tâches de maintenance sur les machines virtuelles. Enfin, un groupes d'utilisateurs ne possédant pas de compte peut utiliser les machines virtuelles pour l'exécution de leurs applications.

Tableau 15-7 illustre le partage possible des composants utilisés et configurés pour l'hôte.

Tableau 15-7. Partage de composants au sein d'un déploiement ouvert à clients multiples

Fonction	Configuration	Commentaires
La console de service partage-t-elle le même réseau physique que les machines virtuelles ?	Non	Isolez la console de service en la configurant sur son propre réseau physique.
La console de service partage-t-elle le même réseau VLAN que les machines virtuelles ?	Non	Isolez la console de service en la configurant sur son propre réseau VLAN. Aucune machine virtuelle et aucun autre outil système (tel que vMotion) ne doit utiliser ce réseau VLAN.
Les machines virtuelles partagent-elles le même réseau physique ?	Oui	Configurez les machines virtuelles sur le même réseau physique.
Existe-t-il un partage de cartes réseau ?	Partage partiel	Isolez la console de service en la configurant sur son propre commutateur virtuel et sur sa propre carte réseau virtuelle. Aucune machine virtuelle, aucun autre outil système ne doit utiliser ce commutateur ou cette carte. Configurez toutes les machines virtuelles sur le même commutateur virtuel et sur la même carte réseau.
Existe-t-il un partage VMFS ?	Oui	Les machines virtuelles peuvent partager des partitions VMFS et leurs fichiers `.vmdk` peuvent résider sur des partitions partagées. Mais les machines virtuelles ne partagent pas de fichiers `.vmdk`.
Niveau de sécurité	Élevé	Permet d'ouvrir les ports de services tels que FTP, en cas de besoin.
Existe-t-il un engagement excessif de la mémoire des machines virtuelles ?	Oui	Configurez une quantité totale de mémoire des machines virtuelles égale à celle de la mémoire physique.

Le Tableau 15-8 illustre la configuration possible des comptes d'utilisateur pour l'hôte.

Tableau 15-8. Configuration de comptes d'utilisateur au sein d'un déploiement ouvert à clients multiples

Catégorie d'utilisateur	Nombre total de comptes
Administrateurs de site	1
Administrateurs clients	10
Administrateurs système	0
Utilisateurs	0

Le Tableau 15-9 indique le niveau d'accès de chaque utilisateur.

Tableau 15-9. Accès des utilisateurs au sein d'un déploiement ouvert à clients multiples

Niveau d'accès	Administrateur de site	Administrateur client	Administrateur système	Utilisateur
Accès racine ?	Oui	Non	Non	Non
Accès par la console de service via SSH ?	Oui	Oui	Non	Non
Accès au Web via vCenter Server et vSphere ?	Oui	Oui	Non	Non
Création et modification de machine virtuelle ?	Oui	Oui	Non	Non
Accès aux machines virtuelles via la console ?	Oui	Oui	Oui	Oui

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 dans ESX, 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]** > **[Général]** 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`

Remarque 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 (cartes 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 adapteur 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 Ouvrez une session sur la console de service et procurez-vous des privilèges racines.

6 Changez les répertoires afin d'accéder au fichier de configuration de la machine virtuelle, dans l'inventaire que vous avez noté à Étape 4.

   Les fichiers de configuration des machines virtuelles se situent dans l'inventaire `/vmfs/volumes/`*`datastore`*, où *datastore* 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 **[Powere 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 ESX 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 (comme 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]** > **[Général]** 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]** > **[Général]** 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 ESX.

Procédure

1 Ouvrez une session sur un système vCenter Server au moyen de 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 Ouvrez une session sur la console de service et procurez-vous des privilèges racines.

5 Changez les répertoires afin d'accéder au fichier de configuration de la machine virtuelle, dans l'inventaire que vous avez noté à Étape 3.

Les fichiers de configuration des machines virtuelles se situent dans l'inventaire `/vmfs/volumes/`*`datastore`*, où *datastore* 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.

Profils d'hôte

Gestion des profils d'hôte 16

La fonction des profils d'hôte crée un profil qui encapsule la configuration de l'hôte et aide à gérer la configuration de l'hôte, surtout dans les environnements où un administrateur gère plus d'un hôte ou d'un cluster dans vCenter Server.

Les profils d'hôte éliminent la configuration par hôte, manuelle ou par l'interface utilisateur de l'hôte et maintiennent l'uniformité et l'exactitude de configuration dans le centre de données en utilisant les règles du profil de l'hôte. Ces règles capturent le plan d'action d'une configuration connue et d'hôte de référence validé et utilisent ceci pour configurer la mise en réseau, le stockage, la sécurité, et d'autres paramètres sur plusieurs hôtes ou clusters. Vous pouvez alors vérifier un hôte ou un cluster par rapport à la configuration d'un profil pour toutes les déviations.

Ce chapitre aborde les rubriques suivantes :

Modèle d'utilisation des profils d'hôte

Cette rubrique décrit le processus d'utilisation des profils d'hôte.

Vous devez avoir installé vSphere avec au moins un hôte correctement configuré.

1 Installez et configurez l'hôte qui sera utilisé comme hôte de référence.

   Un hôte de référence est l'hôte à partir duquel le profil est créé.

2 Créez un profil en utilisant l'hôte de référence indiqué.

3 Attachez un hôte ou un cluster au profil.

4 Vérifiez la conformité de l'hôte par rapport à un profil. Cette opération garantit que l'hôte continue à être configuré correctement.

5 Appliquez le profil de l'hôte de référence aux autres hôtes ou clusters des hôtes.

Remarque Les profils d'hôte sont pris en charge seulement pour les hôtes de VMware vSphere 4.0. Cette fonction n'est pas pris en charge pour les hôtes VI 3.5 ou plus anciens. Si vous avez des hôtes VI de version 3.5 ou précédente gérés par votre vCenter Server 4.0, ce qui suit peut survenir si vous essayez d'utiliser des profils d'hôte pour ces hôtes :

- Vous ne pouvez pas créer un profil d'hôte qui utilise un hôte VMware Infrastructure version 3.5 ou précédente comme hôte de référence.
- Vous ne pouvez pas appliquer un profil d'hôte aux hôtes VI version 3.5 ou précédente. La vérification de conformité échoue.
- Pendant que vous attachez un profil d'hôte à un cluster mixte qui contient des hôtes VI de versions 3.5 ou précédente, la vérification de conformité pour ces hôtes échoue.

En tant que fonction autorisée de vSphere, les profils d'hôte sont disponibles seulement quand la gestion des licences appropriée est en place. Si vous voyez des erreurs, veuillez-vous assurer que vous avez la gestion des licences appropriée de vSphere pour vos hôtes.

Si vous voulez que le profil d'hôte utilise les services d'annuaire pour l'authentification, l'hôte de référence doit être configuré pour utiliser un service d'annuaire. Voir « Configurer un hôte pour utiliser un service d'annuaire », page 196 pour plus d'informations.

Accéder à la vue des profils d'hôte

La vue principale Profils d'hôte répertorie tous les profils disponibles. Les administrateurs peuvent également utiliser la vue principale Profils d'hôte pour effectuer des opérations sur les profils des hôtes et configurer des profils.

La vue principale Profils d'hôte doit être utilisée par des administrateurs expérimentés qui souhaitent effectuer des opérations sur les profils hôtes et configurer des options et des règles avancées. La plupart des opérations telles que la création de nouveaux profils, l'association d'entités et l'application de profils peuvent être effectuées à partir de la vue Hôtes et clusters.

Procédure

- Sélectionnez **[Afficher] > [Gestion] > [Profils hôte]** .

Tous les profils existants sont énumérés sur le côté gauche dans la liste des profils. Quand un profil est sélectionné à partir de la liste de profil, les détails de ce profil sont affichés à droite.

Création d'un profil d'hôte

Vous créez un nouveau profil hôte en utilisant la configuration de l'hôte de référence indiqué.

Un profil d'hôte peut être créé à partir de :

- Vue principale de profil d'hôte
- menu contextuel de l'hôte

Créer un profil d'hôte dans la vue des profils d'hôte

Vous pouvez créer un profil d'hôte à partir de la vue principale Profils d'hôte avec la configuration d'un hôte existant.

Prérequis

Vous devez avoir une installation vSphere et au moins un hôte correctement configuré dans l'inventaire.

Procédure

1 Dans la vue principale Profils d'hôte, cliquez sur **[Créer profil]** .

L'assistant Créer profil s'affiche.

2 Sélectionnez l'option pour créer un nouveau profil et cliquez sur **[Suivant]** .

3 Sélectionnez l'hôte à utiliser pour créer le profil et cliquez sur **[Suivant]** .

4 Tapez le nom et la description du nouveau profil et cliquez sur **[Suivant]** .

5 Passez en revue les informations récapitulatives du nouveau profil et cliquez sur **[Terminer]** pour terminer la création du profil.

Le nouveau profil apparaît dans la liste de profil.

Créer un profil d'hôte à partir d'un hôte

Vous pouvez créer un nouveau profil d'hôte à partir du menu contextuel de l'hôte dans la vue d'inventaire Hôtes et Clusters.

Prérequis

Vous devez avoir une installation vSphere et au moins un hôte correctement configuré dans l'inventaire.

Procédure

1 Dans la vue Hôte et clusters, sélectionnez l'hôte que vous voulez désigner comme l'hôte de référence du nouveau profil d'hôte.

2 Cliquez avec le bouton droit sur l'hôte et sélectionnez **[Profil hôte]** > **[Créer profil à partir de l'hôte]** .

L'assistant Créer profil à partir de l'hôte s'affiche.

3 Tapez le nom et la description du nouveau profil et cliquez sur **[Suivant]** .

4 Passez en revue les informations récapitulatives du nouveau profil et cliquez sur **[Terminer]** pour terminer la création du profil.

Le nouveau profil apparaît dans l'Onglet Résumé de l'hôte.

Exporter un profil d'hôte

Vous pouvez exporter un profil vers un fichier qui est dans le format de profil VMware (`.vpf`).

Remarque Lorsque le profil d'un hôte est exporté, les mots de passe administrateur ne sont pas exportés. C'est une mesure de sécurité et cela empêche que les mots de passe administrateur soient exportés en texte clair lors de l'exportation du profil. Un message vous invitera à saisir à nouveau les valeurs du mot de passe après l'importation du profil et l'attribution d'un mot de passe à un hôte.

Procédure

1 Sur la page principale Profils d'hôte, sélectionnez le profil à exporter dans la liste de profil.

2 Cliquez avec le bouton droit sur le profil et sélectionnez **[Export. profil]** .

3 Sélectionnez l'emplacement et entrez le nom du fichier pour exporter le profil.

4 Cliquez sur **[Enregistrer]** .

Importer un profil d'hôte

Vous pouvez importer un profil à partir d'un fichier dans le format de profil VMware (`.vpf`).

Remarque Lorsque le profil d'un hôte est exporté, les mots de passe administrateur ne sont pas exportés. C'est une mesure de sécurité et cela empêche que les mots de passe administrateur soient exportés en texte clair lors de l'exportation du profil. Un message vous invitera à saisir à nouveau les valeurs du mot de passe après l'importation du profil et l'attribution d'un mot de passe à un hôte.

Procédure

1 Dans la vue principale Profils d'hôte, cliquez sur l'icône **[Créer profil]** .

L'assistant Créer profil s'affiche.

2 Sélectionnez l'option pour importer un profil et cliquez sur **[Suivant]** .

3 Entrez et parcourez le fichier de Format de profil VMware pour importer et cliquez sur **[Suivant]** .

4 Entrez le nom et la description du profil importé et cliquez sur **[Suivant]** lorsque vous avez teminé.

5 Passez en revue les informations récapitulatives du profil importé et cliquez sur **[Terminer]** pour terminer l'importation du profil.

Le profil importé apparaît dans la liste de profil.

Modifier un profil d'hôte

Vous pouvez visualiser et modifier des règles de profil d'hôte, sélection une règle à vérifier pour assurer la conformité, et modifier le nom ou la description de la règle.

Procédure

1 Dans la vue principale Profils d'hôte, sélectionnez le profil à modifier dans la liste de profil.

2 Cliquez sur **[Modifier Profil Hôte]** .

3 (Facultatif) Modifiez le nom ou la description du profil dans les champs en haut de l'éditeur de profil.

4 Modifiez la règle.

5 (Facultatif) Activez ou désactivez la vérification de conformité de la règle.

6 Cliquez sur **[OK]** pour fermer l'éditeur de profil.

Modifier une règle

Une règle décrit comment un paramètre spécifique de configuration devrait être appliqué. L'éditeur de profil permet de modifier les règles appartenant à un profil d'hôte spécifique.

Sur le côté gauche de l'éditeur de profil, vous pouvez dérouler le profil d'hôte. Chaque profil d'hôte se compose de plusieurs sous-profils qui sont indiqués par le groupes fonctionnel pour représenter des instances de configuration. Chaque sous-profil contient de nombreuses règles et de vérifications de conformité qui décrivent la configuration appropriée au profil.

Chaque règle se compose d'une ou plusieurs options qui contient un ou plusieurs paramètres. Les paramètres se composent d'une clé et d'une valeur. La valeur peut correspondre à l'un des types de base, tel qu'un entier, une chaîne, un groupes de chaînes ou un groupes d'entiers.

Les sous-profils (et les règles d'exemple et les vérifications de conformité) qui peuvent être configurés sont :

Tableau 16-1. Configurations de Sous-profil de profil d'hôte

Configuration de Sous-Profil	Règles d'exemple et Vérifications de conformité
Réservation de mémoire	Définissez la réservation de mémoire à une valeur fixe.
Stockage	Configurez le stockage NFS.
Mise en réseau	Configurez un commutateur virtuel, les groupes de ports, la vitesse NIC physique, les règles de sécurité et d'association NIC, le commutateur distribué vNetwork et le port uplink du commutateur distribué vNetwork.
Date et heure	Configurez paramètres de temps, fuseau horaire de serveur.
Pare-feu	Activez ou désactivez un ensemble de règles.
Sécurité	Ajoutez un utilisateur ou un groupes d'utilisateurs, définissez un mot de passe racine.
Service	Configurez les paramètres pour un service.
Avancé	Modifiez les options avancées.

Procédure

1 Ouvrez l'éditeur de profil pour le profil que vous souhaitez modifier.

2 Sur le côté gauche de l'éditeur de profil, déroulez le sous-profil jusqu'à ce que vous atteigniez la règle que vous voulez modifier.

3 Sélectionnez la règle.

Sur le côté droit de l'éditeur de profil, les options et les paramètres de règle sont affichés dans l'onglet Détails de configuration.

4 Sélectionnez une option de règle à partir du menu déroulant et définissez son paramètre.

5 (Facultatif) Si vous modifiez une règle, mais souhaitez revenir à l'option par défaut, cliquez sur **[Revenir]** et l'option est réinitialisée.

Activer la vérification de conformité

Vous pouvez décider de vérifier la conformirté d'une règle de profil d'hôte.

Procédure

1 Ouvrez l'éditeur de profil pour un profil et naviguez à la règle que vous souhaitez activer pour la vérification de conformité.

2 Sur le côté droit de l'éditeur de profil, sélectionnez l'onglet **[Détails conformité]** .

3 Activez la case à cocher pour la règle.

Remarque Si vous désactivez la case à cocher pour que cette règle ne soit pas examinée pour assurer la conformité, les autres règles qui sont activées pour la vérification de conformité seront quand même vérifiées.

Gestion des profils

Après avoir créé un profil d'hôte, vous pouvez gérer le profil en attachant un profil à un hôte ou un cluster particulier, puis en appliquant ce profil sur l'hôte ou le cluster.

Attachement d'entités

Les hôtes qui ont besoin d'être configurés sont attachés à un profil.

Les profils peuvent également être attachés à un cluster. Pour qu'ils soient conformes, tous les hôtes dans un cluster attaché doivent être configurés en fonction du profil. Les hôtes ne sont pas automatiquement configurés en fonction du profil de l'hôte associé au cluster lorsqu'il est ajouté au cluster. Lorsqu'un hôte est ajouté à un cluster qui est associé à un profil, l'hôte est automatiquement associé au profil. Si le profil n'est pas appliqué ou configuré conformément à ce qui est défini dans le profil, cela provoquera l'échec de l'état de conformité pour le profil lors de la prochaine vérification de conformité. Vous corrigez cette erreur en appliquant le profil à l'hôte.

Vous pouvez attacher un hôte ou un cluster à un profil à partir de :

- Vue principale Profils d'hôte
- Menu contextuel de l'hôte
- Menu contextuel du cluster
- Onglet Conformité de profil du cluster

Attacher des entités à partir de la vue des profils d'hôte

Avant de pouvoir appliquer le profil à une entité (hôte ou cluster d'hôtes), vous devez attacher l'entité au profil.

Vous pouvez attacher un hôte ou un cluster à un profil à partir de la vue principale Profils d'hôte.

Procédure

1. Dans la vue principale Profils d'hôte, sélectionnez le profil auquel vous voulez ajouter l'attachement à partir de la liste de profil.
2. Cliquez sur l'icône **[Joindre l'hôte/le cluster]** .
3. Sélectionnez l'hôte ou le cluster de la liste étendue et cliquez sur **[Attacher]** .

   L'hôte ou le cluster est ajouté à la liste Entités Attachées.
4. (Facultatif) Cliquez sur **[Détacher]** pour supprimer un attachement à partir d'un hôte ou d'un cluster.
5. Cliquez sur **[OK]** pour fermer le dialogue.

Attacher des entités à partir de l'hôte

Avant de pouvoir appliquer le profil à un hôte, vous devez attacher l'hôte au profil.

Vous pouvez attacher un profil à un hôte à partir du menu contextuel de l'hôte dans la vue d'inventaire Hôtes et Clusters.

Procédure

1 Dans la vue Hôte et clusters, sélectionnez l'hôte auquel vous voulez attacher un profil.

2 Cliquez avec le bouton droit sur l'hôte et sélectionnez **[Profil hôte] > [Gérer profil]** .

REMARQUE Si aucun profil d'hôte n'existe dans votre inventaire, un dialogue s'affiche demandant si vous voulez créer et attacher l'hôte à ce profil.

3 Dans le dialogue Attach Profile, sélectionnez le profil à attacher à l'hôte et cliquez sur **[OK]** .

Le profil d'hôte est mis à niveau dans l'onglet **[Résumé]** de l'hôte.

Application des profils

Pour amener un hôte à l'état désiré comme spécifié dans le profil, appliquez le profil à l'hôte.

Vous pouvez appliquer un profil à un hôte à partir de :

- Vue principale Profils d'hôte
- Menu contextuel de l'hôte
- Onglet Conformité de profil du cluster

Appliquer un profil à partir de la vue des profils d'hôte

Vous pouvez appliquer un profil à un hôte à partir de la vue principale Profils d'hôte.

Prérequis

L'hôte doit être en mode maintenance avant qu'un profil ne lui soit appliqué.

Procédure

1 Dans la vue principale Profils d'hôte, sélectionnez le profil que vous voulez appliquer à l'hôte.

2 Sélectionnez l'onglet **[Hôtes et clusters]** .

La liste des hôtes joints est affiché sous Nom d'entité.

3 Cliquez sur **[Appliquer le profil]** .

Dans l'éditeur de profil, vous pourriez être invité à entrer les paramètres requis pour appliquer le profil.

4 Entrez les paramètres et cliquez sur **[Suivant]** .

5 Continuer jusqu'à ce que tous les paramètres nécessaires soient entrés.

6 Cliquez sur **[Terminer]** .

Le statut de conformité est mis à niveau.

Appliquer un profil à partir de l'hôte

Vous pouvez appliquer un profil à un hôte à partir du menu contextuel de l'hôte.

Prérequis

L'hôte doit être en mode maintenance avant d'être appliqué à un profil

Procédure

1 Dans la vue Hôte et clusters, sélectionnez l'hôte auquel vous voulez appliquer un profil.

2 Cliquez avec le bouton droit sur l'hôte et sélectionnez **[Profil hôte] > [Appliquer le profil]** .

3 Dans Profile Editor, entrez les paramètres et cliquez sur **[Suivant]** .

4 Continuer jusqu'à ce que tous les paramètres nécessaires soient entrés.

5 Cliquez sur **[Terminer]** .

Le statut de conformité est mis à niveau.

Changer l'hôte de référence

La configuration de l'hôte de référence est utilisée pour créer le profil d'hôte..

Vous pouvez effectuer cette tâche à partir de la vue principale Profils d'hôte ou du menu contextuel de l'hôte.

Prérequis

Le profil d'hôte doit déjà exister.

Procédure

1 Vous pouvez effectuer cette tâche soit à partir de la vue principale Profils d'hôte ou à partir de l'hôte.

- Dans la vue principale Profils d'hôte, cliquez avec le bouton droit sur le profil dont vous souhaitez modifier l'hôte de référence et sélectionnez **[Changer l'hôte de référence]** .
- Dans la vue Hôtes et Clusters, cliquez avec le bouton droit sur l'hôte duquel vous voulez mettre à niveau les références et sélectionnez **[Gérer les profils]** .

Le dialogue Detach or Change Host Profile s'affiche.

2 Déterminez si vous voulez détacher le profil à partir de l'hôte ou du cluster ou modifiez l'hôte de référence du profil.

- Cliquez sur **[Détacher]** pour supprimer l'association entre l'hôte et le profil.
- Cliquez sur **[Modifier]** pour continuer la mise à niveau de l'hôte de référence du profil.

Si vous sélectionnez **[Modifier]** ,le dialogue Attach Profile s'affiche. L'hôte actuel auquel le profil fait référence est affiché comme **[Hôte référence]** .

3 Augmentez la liste d'inventaire et sélectionnez l'hôte auquel vous voulez joindre le profil.

4 Cliquez sur **[Mise à niveau]** .

L' **[Hôte référence]** est mis à niveau.

5 Cliquez sur **[OK]** .

L'onglet Résumé du profil d'hôte énumère l'hôte de référence mis à niveau.

Gérer les profils d'un cluster

Vous pouvez créer un profil, attacher un profil ou mettre à niveau des hôtes de référence à partir du menu contextuel du cluster.

Procédure

- Dans la vue Hôtes et Clusters, cliquez avec le bouton droit sur un cluster et sélectionnez **[Profil hôte] > [Gérer profil]** . Selon la configuration du profil d'hôte, les résultats sont les suivants :

Etat du profil et tâche	Résultat
Si le cluster n'est pas lié à un profil d'hôte et qu'aucun profil n'existe dans l'inventaire, créez un profil.	a Une boîte de dialogue demande si vous voulez créer un profil et le lier au cluster. b Si vous sélectionnez **[Oui]** , l'assistant Créer un profil s'affiche.
Si le cluster n'est pas lié à un profil d'hôte et qu'un ou plusieurs profils existent dans l'inventaire, liez un profil.	a Le dialogue Joindre le profil s'ouvre. b Sélectionnez le profil à associer au cluster et cliquez sur **[OK.]**
Si le cluster est déjà lié à un profil d'hôte, détachez le profil ou liez le cluster à un profil différent.	Dans la boîte de dialogue, cliquez sur **[Détacher]** pour détacher le profil du cluster ou sur **[Modifier]** pour lier un profil différent au cluster.

Mise à niveau des profils à partir de l'hôte de référence

Si la configuration de l'hôte (l'hôte de référence) à partir duquel un profil a été créé change, vous pouvez mettre le profil à niveau pour que sa configuration corresponde à la configuration de l'hôte de référence.

Une fois que vous créez un profil d'hôte, des mises à niveau incrémentielles risquent d'être nécessaires pour le profil. Vous pouvez le faire par l'intermédiaire de deux méthodes :

- Faites les modifications de configuration sur l'hôte de référence dans vSphere Client, puis mettez le profil de l'hôte de référence à niveau. Les paramètres du profil existant sont mis à niveau pour correspondre à ceux de l'hôte de référence.
- Mettez le profil à niveau via l'éditeur de profil.

Alors que la mise à niveau du profil à partir de l'éditeur de profil est plus complète et donne plus d'options, mettre le profil à niveau à partir de l'hôte de référence permet de valider la configuration avant de la diffuser sur les d'autres hôtes attachés au profil.

La mise à niveau du profil à partir de l'hôte de référence est effectuée dans la vue principale Profils d'hôte.

Procédure

- Dans la vue principale Profils d'hôte, cliquez avec le bouton droit sur le profil que vous souhaitez mettre à niveau et sélectionnez **[Mise à niveau profil depuis Hôte Référence]** .

Vérification de la conformité

Vérifier la conformité garantit que l'hôte ou le cluster continue à être configuré correctement.

Après la configuration d'un hôte ou d'un cluster avec le profil de l'hôte de référence, un changement manuel, par exemple, peut survenir et rendre la configuration incorrecte. Vérifier la conformité sur une base régulière garantit que l'hôte ou le cluster continue à être configuré correctement.

Vérification de conformité à partir de la vue des profils d'hôte

Vous pouvez vérifier la conformité d'un hôte ou d'un cluster sur un profil à partir de la vue principale Profils d'hôte.

Procédure

1 À partir de la liste Profils d'hôte, sélectionnez le profil que vous voulez vérifier.

2 Dans l'onglet **[Hôtes et clusters]** , sélection l'hôte ou le cluster à partir de la liste sous Nom Entité.

3 Cliquez sur **[Vérifier la conformité maintenant]** .

L'état de conformité est mis à niveau en Conforme, Inconnu, ou Non conforme.

Si l'état de conformité est non conforme, vous pouvez appliquer l'hôte au profil.

Vérification de conformité à partir de l'hôte

Après avoir attaché un profil à un hôte, exécutez une vérification de conformité à partit du menu contextuel de l'hôte pour vérifier la configuration.

Procédure

1 Dans la vue Hôte et clusters, sélectionnez l'hôte sur lequel vous voulez exécuter la vérification de conformité.

2 Cliquez avec le bouton droit sur l'hôte et sélectionnez **[Profil hôte] > [Contrôler la conformité]** .

L'état de conformité de l'hôte est affiché dans l'onglet **[Résumé]** de l'hôte.

Si l'hôte n'est pas conforme, vous devez appliquer le profil à l'hôte.

Vérification de conformité du cluster

Un cluster peut être vérifié pour la conformité avec un profil d'hôte ou dans des conditions et des paramètres spécifiques de cluster.

Procédure

1 Dans la vue Hôte et clusters, sélectionnez le cluster sur lequel vous voulez exécuter la vérification de conformité.

2 Dans l'onglet Conformité de profil, cliquez sur **[Vérifier la conformité maintenant]** pour vérifier la conformité du cluster avec à la fois le profil d'hôte qui est attaché à ce cluster et aux conditions de cluster, si applicable.

- Le cluster est vérifié pour assurer la conformité aux paramètres spécifiques pour des hôtes dans le cluster, tel que DRS, HA, et DPM. Par exemple, il peut vérifier si vMotion est activé. L'état de conformité pour les conditions de cluster est mis à niveau. Cette vérification est effectuée même si un profil d'hôte n'est pas attaché au cluster.
- Si un profil d'hôte est attaché au cluster, le cluster est vérifié pour assurer la conformité au profil d'hôte. L'état de conformité pour le profil d'hôte est mis à niveau.

3 (Facultatif) Cliquez sur **[Description]** à côté des Conditions Cluster pour une liste des conditions de cluster spécifiques.

4 (Facultatif) Cliquez sur **[Description]** à côté des Profils d'hôte pour une liste de vérifications de conformité de profil d'hôte spécifiques.

5 (Facultatif) Cliquez sur **[Modifier]** pour modifier le profil d'hôte qui est attaché au cluster.

6 (Facultatif) Cliquez sur **[Supprimer]** pour détacher le profil d'hôte qui est attaché au cluster.

Si le cluster n'est pas conforme, le profil doit être appliqué séparément à chaque hôte dans le cluster.

Annexes

Commandes de support technique ESX

A

La plupart des commandes de cette annexe sont réservées à l'utilisation de support technique et incluses uniquement pour référence. Toutefois, dans quelques cas, ces commandes sont le seul moyen d'exécuter une tâche de configuration pour l'hôte. Aussi, si vous perdez la connexion à votre hôte, l'exécution de certaines de ces commandes via l'interface de ligne de commande peut être votre unique recours (par exemple, si la mise en réseau devient non fonctionnelle et l'accès au vSphere Client n'est par conséquent pas disponible).

Remarque Si vous utilisez les commandes dans cette annexe, vous devez exécuter la commande `service mgmt-vmware restart` pour redémarrer le processus `vmware-hostd` et alerter le vSphere Client et d'autres outils de gestion que la configuration a changé. En règle générale, évitez d'exécuter les commandes de cette annexe si l'hôte se trouve actuellement sous la gestion du vSphere Client ou de vCenter Server.

L'interface utilisateur graphique du vSphere Client fournit les moyens préférés d'exécution de tâches de configuration décrites dans cette section. Vous pouvez utiliser cette rubrique pour connaître les commandes du vSphere Client à utiliser à la place de ces commandes. Cette section propose un résumé des actions que vous effectuez dans vSphere Client mais ne donne pas d'instructions complètes. Pour des détails sur l'utilisation des commandes et l'exécution de tâches de configuration via le vSphere Client, consultez l'aide en ligne.

Vous pouvez trouver des informations complémentaires sur plusieurs commandes ESX en vous connectant à la console de service et en utilisant la commande `man <esxcfg_command_name>` pour afficher les pages principales.

Tableau A-1 répertorie les commandes de support technique fournies pour ESX, résume la fonction de chaque commande et propose une alternative au vSphere Client. Vous pouvez effectuer la plupart des actions du vSphere Client listées dans le tableau seulement après avoir sélectionné un hôte ESX à partir du panneau d'inventaire et cliqué sur l'onglet **[Configuration]** . Ces actions sont préliminaires à toute procédure évoquée ci-dessous, sauf indication contraire.

Tableau A-1. Commandes de support technique ESX

Commande	Fonction de la commande et procédure du vSphere Client
`esxcfg-advcfg`	Configure les options avancées pour ESX. Pour configurer les options avancées dans vSphere Client, cliquez sur **[Paramètres avancés]** . Lorsque la boîte de dialogue Paramètres avancés s'ouvre, utilisez la liste à gauche pour sélection le type de périphérique ou l'activité que vous souhaitez utiliser, puis entrez les paramètres appropriés.
`esxcfg-auth`	Configure l'authentification. Vous pouvez utiliser cette commande pour basculer entre les plug-ins `pam_cracklib.so` et `pam_passwdqc.so` afin de mettre en application la règle de changement de mot de passe. Vous utilisez aussi cette commande pour réinitialiser les options de ces deux plug-ins. Il n'existe aucun moyen de configurer ces fonctions dans le vSphere Client.

Tableau A-1. Commandes de support technique ESX (suite)

Commande	Fonction de la commande et procédure du vSphere Client
`esxcfg-boot`	Configure les paramètres d'amorce. Cette commande est utilisée dans le processus d'amorce et elle est réservée à l'assistance technique de VMware. Ne lancez pas cette commande à moins d'y être invité par un représentant de l'assistance technique de VMware. Il n'existe aucun moyen de configurer ces fonctions dans vSphere Client.
`esxcfg-dumppart`	Configure une partition de diagnostic ou recherche des partitions de diagnostic existantes. Lorsque vous installez ESX, une partition de diagnostic est créée pour stocker les informations de débogage dans l'éventualité d'une défaillance système. Vous n'avez pas besoin de créer cette partition manuellement à moins que vous ne déterminiez qu'il n'existe aucune partition de diagnostic pour l'hôte. Vous pouvez effectuer les activités de gestion suivantes pour les partitions de diagnostic dans vSphere Client : ■ Déterminer s'il existe une partition de diagnostic : cliquez sur **[Stockage]** > **[Ajouter stockage]** et vérifiez la première page de l'assistant **[Ajouter stockage]** pour voir si elle contient l'option **[Diagnostic]**. Si **[Diagnostic]** ne fait pas partie des options, ESX dispose déjà d'une partition de diagnostic. ■ Configurer une partition de diagnostic : cliquez sur **[Stockage]** > **[Ajouter stockage]** > **[Diagnostic]** et évoluez à travers l'assistant.
`esxcfg-firewall`	Configure les ports de pare-feu de la console de service. Afin de configurer les ports de pare-feu pour des agents et services pris en charge dans vSphere Client, vous sélectionnez les services Internet qui seront autorisés à accéder à l'hôte ESX. Cliquez sur **[Profil de sécurité]** > **[Pare-feu]** > **[Propriétés]** et utilisez la boîte de dialogue **[Propriétés de pare-feu]** pour ajouter des services. Vous pouvez configurer des services non pris en charge via le vSphere Client. Pour ces services, utilisez la commande `esxcfg-firewall`.
`esxcfg-info`	Imprimez les informations sur l'état de la console de service, VMkernel, les divers sous-systèmes du réseau virtuel et le matériel de ressources de stockage. vSphere Client ne propose pas de méthode pour imprimer ces informations, mais vous pouvez en obtenir au travers des différents onglets et fonctions dans l'interface utilisateur. Par exemple, vous pouvez contrôler le statut de vos machines virtuelles en consultant les informations dans l'onglet **[Machines virtuelles]**.
`esxcfg-init`	Effectue des routines d'initialisation interne. Cette commande est utilisée dans le processus d'amorce et ne doit en aucun cas être employée. Cette commande peut causer des problèmes pour ESX. Il n'existe pas d'équivalent pour cette commande avec le vSphere Client.
`esxcfg-module`	Règle les paramètres de pilote et modifie les pilotes à charger durant le démarrage. Cette commande est utilisée dans le processus d'amorce et elle est réservée à l'assistance technique de VMware. Ne lancez pas cette commande à moins d'y être invité par un représentant de l'assistance technique de VMware. Il n'existe pas d'équivalent pour cette commande avec le vSphere Client.
`esxcfg-mpath`	Configure les paramètres multichemins pour vos disques iSCSI ou Fibre Channel. Afin de configurer les paramètres multichemins pour votre stockage dans vSphere Client, cliquez sur **[Stockage]**. Sélectionnez une banque de données ou un LUN mappé et cliquez sur **[Propriétés]**. Lorsque la boîte de dialogue **[Propriétés]** apparaît, sélectionnez l'extension souhaitée, si nécessaire. Cliquez ensuite sur **[Périphérique de domaine]** > **[Gérer les chemins]** et utilisez la boîte de dialogue **[Gérer les chemins]** pour configurer les chemins.

Tableau A-1. Commandes de support technique ESX (suite)

Commande	Fonction de la commande et procédure du vSphere Client
`esxcfg-nas`	Gère les montages NFS. Vous utilisez cette commande pour créer ou démonter une banque de données NFS. Pour consulter les banque de données NFS dans vSphere Client, cliquez sur **[Stockage > Banque de données]** et parcourez la liste de banque de données. Vous pouvez également effectuer les activités suivantes depuis la vue **[Stockage > Banque de données]** : ■ Afficher les attributs d'une banque de données NFS : cliquez sur la banque de données et consultez les informations sous **[Détails]** . ■ Créer une banque de données NFS : cliquez sur **[Ajouter stockage]** . ■ Démonter une banque de données NFS : cliquez sur **[Supprimer]** , ou cliquez avec le bouton droit sur la banque de données à démonter et sélectionnez **[Démonter]** .
`esxcfg-nics`	Imprime la liste de adaptateurs réseau physiques ainsi que les informations sur le pilote, le périphérique PCI et l'état de liaison de chaque carte d'interface réseau. Vous pouvez aussi utiliser cette commande pour contrôler le duplexage et la vitesse d'un adapteur réseau physique. Pour afficher les informations des adaptateurs réseau physiques de l'hôte dans vSphere Client, cliquez sur **[Adaptateurs réseau]** . Pour modifier la vitesse et le duplexage d'un adapteur réseau physique dans vSphere Client, cliquez sur **[Mise en réseau]** > **[Propriétés]** pour tout commutateur virtuel associé à la carte réseau physique. Dans la boîte de dialogue **[Propriétés]** , cliquez sur **[Adaptateurs réseau]** > **[Modifier]** et sélectionnez la combinaison de duplex et de vitesse.
`esxcfg-resgrp`	Restaure les paramètres de groupes de ressources et permet d'effectuer une gestion de groupes de ressources basique. Sélectionnez un pool de ressources à partir du panneau d'inventaire et cliquez sur **[Modifier les paramètres]** dans l'onglet **[Résumé]** pour modifier les paramètres de groupes de ressources.
`esxcfg-route`	Règle ou récupère l'itinéraire de la passerelle VMkernel par défaut, et ajoute, supprime ou liste les itinéraires statiques. Pour afficher l'itinéraire de la passerelle VMkernel par défaut dans vSphere Client, cliquez sur **[DNS et routage]** . Pour modifier l'itinéraire par défaut, cliquez sur **[Propriétés]** et mettez les informations à niveau dans les deux onglets de la boîte de dialogue **[DNS et configuration de routage]** .
`esxcfg-swiscsi`	Configure votre carte iSCSI logiciel. Pour configurer votre système iSCSI logiciel dans vSphere Client, cliquez sur **[Adaptateurs de stockage]** , sélectionnez la carte iSCSI que vous souhaitez configurer et cliquez sur **[Propriétés]** . Utilisez la boîte de dialogue **[Propriétés initiateur iSCSI]** pour configurer la carte.
`esxcfg-upgrade`	Met à niveau depuis ESX Server 2.x à ESX Server 3.x. Cette commande n'est pas destinée à une utilisation générale. Vous complétez les trois tâches suivantes lorsque vous passez d'une version 2.x à 3.x. Certaines actions peuvent être effectuées dans vSphere Client : ■ Mettre l'hôte à niveau : vous mettez les fichiers binaires à niveau en passant d'ESX Server 2.x à ESX Server 3.x. Vous ne pouvez pas effectuer cette étape depuis le vSphere Client. ■ Mettre le système de fichiers à niveau : pour passer de VMFS-2 à VMFS-3, interrompez ou mettez hors tension vos machines virtuelles, puis cliquez sur **[Inventaire]** > **[Hôte]** > **[Entrer mode maintenance]** . Cliquez sur **[Stockage]** , sélectionnez un périphérique de stockage et cliquez sur **[Mise à niveau à VMFS-3]** . Vous devez effectuer cette étape pour chaque périphérique de stockage que vous souhaitez mettre à niveau. ■ Mettre les machines virtuelles à niveau : pour mettre les machines virtuelles à niveau d'une version VMS-2 à VMS-3, cliquez avec le bouton droit sur la machine virtuelle dans le panneau d'inventaire et choisissez **[Mettre à niveau la machine virtuelle]** .

Tableau A-1. Commandes de support technique ESX (suite)

Commande	Fonction de la commande et procédure du vSphere Client
`esxcfg-scsidevs`	Imprime un adapteur des périphériques de stockage VMkernel pour les périphériques de console de service. Il n'existe pas d'équivalent pour cette commande avec le vSphere Client.
`esxcfg-vmknic`	Crée et met à niveau les paramètres VMkernel TCP/IP pour vMotion, NAS et iSCSI. Pour configurer les connexions réseau de vMotion, NFS ou iSCSI dans vSphere Client, cliquez sur **[Gestion de réseaux > Ajouter gestion réseau]** . Sélectionnez **[VMkernel]** et évoluez à travers l' **[Assistant Ajouter réseau]** . Définissez le masque de sous-réseau, l'adresse IP et la passerelle par défaut VMkernel à l'étape **[Paramètres de connexion]** . Pour consulter vos paramètres, cliquez sur l'icône bleu à gauche du port NFS, iSCSI ou vMotion. Pour modifier l'un de ces paramètres, cliquez sur **[Propriétés]** pour le commutateur. Sélectionnez le port dans la liste de la boîte de dialogue **[Propriétés]** du commutateur et cliquez sur **[Modifier]** pour ouvrir la boîte de dialogue **[Propriétés]** du port et modifier ses paramètres.
`esxcfg-vswif`	Crée et met à niveau les paramètres réseau de la console de service. Utilisez cette commande si vous ne pouvez pas gérer l'hôte ESX via le vSphere Client en raison de problèmes de configuration réseau. Pour configurer les connexions de la console de service dans vSphere Client, cliquez sur **[Gestion de réseaux > Ajouter gestion réseau]** . Sélectionnez **[Console de service]** et parcourez les étapes de l'assistant Ajouter réseau. Définissez le masque de sous-réseau, l'adresse IP et la passerelle par défaut de la console de service à l'étape **[Paramètres de connexion]** . Pour consulter vos paramètres, cliquez sur l'icône bleu à gauche du port de la console de service. Pour modifier l'un de ces paramètres, cliquez sur **[Propriétés]** pour le commutateur. Sélectionnez le port de la console de service à partir de la liste dans la boîte de dialogue **[Propriétés]** du commutateur. Cliquez sur **[Modifier]** pour ouvrir la boîte de dialogue **[Propriétés]** du port et modifier ses paramètres.
`esxcfg-vswitch`	Crée et met à niveau les paramètres réseau de la machine virtuelle. Pour configurer les connexions d'une machine virtuelle dans vSphere Client, cliquez sur **[Gestion de réseaux > Ajouter gestion réseau]** . Sélectionnez **[Machine virtuelle]** et évoluez à travers l' **[Assistant Ajouter réseau]** . Pour consulter vos paramètres, cliquez sur l'icône bleu à gauche du port de la machine virtuelle. Pour modifier l'un de ces paramètres, cliquez sur **[Propriétés]** pour le commutateur. Sélectionnez le port dans la liste de la boîte de dialogue **[Propriétés]** du commutateur et cliquez sur **[Modifier]** pour ouvrir la boîte de dialogue **[Propriétés]** du port et modifier ses paramètres.

Commandes Linux utilisées avec ESX

B

Pour faciliter certaines opérations internes, les installations ESX comportent un sous-ensemble de commandes de configurations Linux standard, comme par exemple, des commandes de configuration de stockage et de réseau. L'utilisation de ces commandes pour effectuer des tâches de configuration peut entraîner de sérieux conflits de configuration et rendre certaines fonctions ESX inutilisables.

Travaillez toujours via le vSphere Client lorsque vous configurez ESX, sauf si la documentation vSphere ou l'assistance technique de VMware vous a invité à procéder autrement.

Utilisation de vmkfstools

C

L'utilitaire `vmkfstools` permet de créer et de manipuler des disques virtuels, des systèmes de fichiers, des volumes logiques et des périphériques de stockage physiques sur les hôtes VMware ESX.

Grâce à `vmkfstools`, vous pouvez créer et gérer un système de fichiers de machine virtuelle (VMFS) sur une partition physique de disque. Vous pouvez également utiliser cette commande pour manipuler des fichiers (fichiers de disque virtuels, par exemple) stockés sur VMFS-2, VMFS-3 et NFS.

Vous pouvez effectuer la plupat des opérations `vmkfstools` via vSphere Client.

Cette annexe aborde les rubriques suivantes :

Syntaxe des commandes vmkfstools

En règle générale, vous n'avez pas besoin de vous connecter en tant qu'utilisateur racine pour pouvoir exécuter les commandes `vmkfstools`. Toutefois, certaines commandes (telles que les commandes de système de fichiers) peuvent nécessiter une connexion d'utilisateur racine.

Avec les commandes `vmkfstools`, utilisez les arguments suivants :

- *options* : options de ligne de commande et arguments associés, utilisés pour spécifier l'activité de `vmkfstools` (choix du format de disque lors de la création d'un disque virtuel, par exemple).

  Une fois que vous avez entré cette option, vous devez spécifier un fichier ou un système de fichiers VMFS sur lequel l'opération sera effectuée. Pour cela, entrez un chemin d'accès (relatif ou absolu) dans la hiérarchie `/vmfs`.

- *partition* : permet de spécifier des partitions de disque. Cet argument utilise un format `vml.`*`vml_ID`*`:P` , où *vml_ID* correspond à l'ID de périphérique renvoyé par la baie de stockage et `P` correspond à un nombre entier représentant le numéro de partition. Le numéro de partition doit être supérieur à zéro (0) et correspondre à une partition VMFS valide de type `fb`.

- *device* : permet de spécifier des périphériques ou des volumes logiques. Cet argument utilise un chemin du système de fichiers de périphérique ESX. Il commence par `/vmfs/devices`, ce qui correspond au point de montage du système de fichier du périphérique.

Lorsque vous spécifiez différents types de périphériques, utilisez les formats suivants :

- `/vmfs/devices/disks` pour les disques locaux ou SAN.
- `/vmfs/devices/lvm` pour les volumes logiques ESX.
- `/vmfs/devices/generic` pour les périphériques SCSI génériques (lecteurs de bande, par exemple).

- *path* permet de spécifier un système de fichiers VMFS ou un fichier. Cet argument est un chemin absolu ou relatif désignant un lien symbolique d'accès à un répertoire, à un mappage de périphérique brut ou à un fichier situé sous `/vmfs`.
  - Pour spécifier un système de fichiers VMFS, utilisez le format suivant :

    `/vmfs/volumes/`*`file_system_UUID`*

    ou

    `/vmfs/volumes/`*`file_system_label`*
  - Pour spécifier un fichier VMFS, utilisez le format suivant :

    `/vmfs/volumes/`*`file system label`*`/`*`file system UUID`*`/[dir]/myDisk.vmdk`

    Il est inutile d'entrer le chemin d'accès complet si l'inventaire de travail en cours d'utilisation est l'inventaire parent de `myDisk.vmdk`.

    Par exemple,

    `/vmfs/volumes/datastore1/rh9.vmdk`

Options vmkfstools

La commande `vmkfstools` se compose de différentes options. Certaines d'entre elles s'adressent uniquement aux utilisateurs avancés.

Vous pouvez spécifier le format long ou le format à lettre unique, au choix. Par exemple, les commandes suivantes sont identiques :

```
vmkfstools --createfs vmfs3 --blocksize 2m vml.vml_ID:1
vmkfstools -C vmfs3 -b 2m vml.vml_ID:1
```

Sous-option -v

La sous-option `-v` indique le niveau de verbosité du résultat de la commande.

Le format de cette sous-option est le suivant :

`-v --verbose` *`number`*

Pour spécifier la valeur *`number`*, utilisez un nombre entier compris entre 1 et 10.

Vous pouvez spécifier la valeur de la sous-option `-v` via l'option `vmkfstools` de votre choix. Si le résultat de l'option n'est pas utilisable avec la sous-option `-v`, `vmkfstools` ignore `-v`.

Remarque Puisque vous pouvez inclure la sous-option `-v` dans toute ligne de commande `vmkfstools`, `-v` n'est pas mentionnée dans les descriptions d'options.

Options de système de fichiers

Les options de système de fichier permettent de créer un système de fichiers VMFS. Ces options ne s'appliquent pas à NFS. Vous pouvez exécuter un grand nombre de ces tâches via vSphere Client.

Création d'un système de fichier VMFS

Pour créer un système de fichiers VMFS, utilisez la commande `vmkfstools`.

```
-C --createfs vmfs3
      -b --blocksize block_sizekK|mM
      -S --setfsname fsName
```

Cette option permet de créer un système de fichiers VMFS-3 sur la partition SCSI spécifiée (comme par exemple `vml.vml_ID:1`). Cette partition devient alors la partition principale du système de fichiers.

Les systèmes de fichiers VMFS-2 sont en lecture seule sur les hôtes ESX. Vous ne pouvez ni créer ni modifier les systèmes de fichiers VMFS-2, mais vous pouvez lire les fichiers qui y sont stockés. Les systèmes de fichiers VMFS-3 ne sont pas accessibles à partir des hôtes ESX 2.x.

AVERTISSEMENT Vous ne pouvez disposer que d'un volume VMFS par LUN.

Vous pouvez spécifier les sous-options suivantes avec l'option `-C` :

- `-b --blocksize` – Définit la taille de bloc applicable au système de fichiers VMFS-3. La taille de bloc par défaut est égale à 1 Mo. La valeur de *block_size* spécifiée doit être un multiple de 128 ko (valeur minimale : 128 ko). Lorsque vous entrez une taille, indiquez le type d'unité en ajoutant un suffixe m or M. Le type d'unité ne respecte pas la casse. `vmkfstools` considère que le suffixe m ou M signifie méga-octets et que le suffixe k ou K signifie kilo-octets.
- `-S --setfsname` – Définit l'étiquette d'un volume VMFS appartenant au système de fichiers VMFS-3 créé. Vous ne devez utiliser cette sous-option qu'avec l'option `-C`. L'étiquette spécifiée peut comporter au maximum 128 caractères ; elle ne doit pas contenir d'espaces au début ou à la fin.

  Une fois que vous avez défini une étiquette de volume, vous pouvez l'utiliser lorsque vous spécifiez le volume VMFS pour la commande `vmkfstools`. L'étiquette de volume apparaît dans les listes générées pour la commande Linux `ls -l` et sous forme de lien symbolique d'accès au volume VMFS dans l'inventaire `/vmfs/volumes`.

  Pour modifier l'étiquette de volume VMFS, utilisez la commande Linux `ln -sf`. En voici un exemple :

  `ln -sf /vmfs/volumes/UUID /vmfs/volumes/fsName`

  fsName correspond à la nouvelle étiquette de volume à utiliser pour le volume VMFS *UUID*.

Exemple de création d'un système de fichiers VMFS

Cet exemple illustre la création d'un nouveau système de fichiers VMFS-3 (my_vmfs) dans la partition `vml.vml_ID:1`. La taille de bloc de ce système de fichiers est égale à 1 Mo.

`vmkfstools -C vmfs3 -b 1m -S my_vmfs /vmfs/devices/disks/vml.vml_ID:1`

Extension d'un volume VMFS-3 existant

Pour ajouter une extension à un volume VMFS, utilisez la commande `vmkfstools`.

`-Z --extendfs extention-device existing-VMFS-volume`

Cette option permet d'ajouter une autre extension à un volume VMFS créé précédemment (*existing-VMFS-volume*). Vous devez spécifier le chemin complet (par exemple `/vmfs/devices/disks/vml.vml_ID:1`), et pas uniquement le nom court (`vml.vml_ID:1`). Chaque fois que vous utilisez cette option, vous ajoutez une extension à un volume VMFS-3, qui s'étend alors sur plusieurs partitions. Un volume VMFS-3 logique peut avoir au maximum 32 extensions physiques.

AVERTISSEMENT Lorsque vous utilisez cette option, vous perdez les données présentes sur le périphérique SCSI spécifié dans *extension-device*.

Exemple d'extension d'un volume VMFS-3

Cet exemple illustre l'extension du système de fichiers logique sur une nouvelle partition.

```
vmkfstools -Z /vmfs/devices/disks/vml.vml_ID_2:1
/vmfs/devices/disks/vml.vml_ID_1:1
```

Le système de fichiers s'étend désormais sur deux partitions—`vml.vml_ID_1:1` et `vml.vml_ID_2:2`. Dans cet exemple, `vml.vml_ID_1:1` correspond au nom de la partition principale.

Liste d'attributs d'un volume VMFS

Pour répertorier les attributs applicables à un volume VMFS, utilisez la commande `vmkfstools`.

```
-P --queryfs
     -h --human-readable
```

Lorsque vous utilisez cette option pour un fichier ou répertoire de volume VMFS, l'option répertorie les attributs du volume spécifié. Les attributs répertoriés incluent le numéro de version VMFS (VMFS 2 ou VMFS-3), le nombre d'extensions comprenant le volume VMFS spécifié, l'étiquette de volume (le cas échéant), l'UUID et la liste des noms de périphériques sur lesquels réside chaque extension.

REMARQUE Si l'un des périphériques hébergeant le système de fichiers VMFS est mis hors tension, le nombre d'extension et l'espace disponible sont modifiés en conséquence.

Vous pouvez spécifier la valeur de la sous-option `-h` via l'option `-P`. Dans ce cas, `vmkfstools` indique la capacité du volume sous une forme plus lisible (par exemple `5k`, `12.1M`, ou `2.1G`).

Mise à niveau d'un disque virtuel VMFS-2 vers VMFS-3

Vous pouvez mettre à niveau un système de fichiers VMFS-2 vers VMFS-3.

AVERTISSEMENT La conversion VMFS-2 à VMFS-3 est un processus à sens unique. Une fois que vous avez converti un volume VMFS-2 en volume VMFS-3, vous ne pouvez pas le reconvertir en volume VMFS-2.

Vous ne pouvez mettre à niveau un système de fichiers VMFS-2 que si sa taille de bloc ne dépasse pas 8 Mo.

Lorsque vous mettez à niveau le système de fichiers, utilisez les options suivantes :

- `-T --tovmfs3 -x --upgradetype [zeroedthick|eagerzeroedthick|thin]`

  Cette option permet de convertir un système de fichiers VMFS-2 en système VMFS-3 en conservant tous les fichiers du système de fichiers. Avant la conversion, déchargez les pilotes `vmfs2` et `vmfs3` et chargez le pilote du système de fichier auxiliaire (`fsaux`), avec l'option de module `fsauxFunction=upgrade`.

Vous devez spécifier le type de mise à niveau à l'aide de l'une des sous-options `-x --upgradetype` suivantes :

- `-x zeroedthick` (valeur par défaut) – Permet de conserver les propriétés des fichiers épais VMFS-2. Avec le format `zeroedthick`, l'espace disque est alloué aux fichiers en vue d'une utilisation ultérieure, et les blocs de données non utilisés ne sont pas mis à zéro.
- `-x eagerzeroedthick` – Permet de mettre à zéro les blocs de données non utilisés dans les fichiers épais au cours de la conversion. Si vous utilisez cette sous-option, le processus de mise à niveau peut être plus long qu'avec les autres options.
- `-x thin` – Permet de convertir les fichiers épais VMFS-2 en fichiers légers VMFS-3. Contrairement au format `thick`, le format léger ne permet pas d'allouer aux fichiers un espace supplémentaire en vue d'une utilisation future. Cet espace supplémentaire est alloué sur demande. Pendant la conversion, les blocs non utilisés des fichiers `thick` sont ignorés.

De même, pendant cette opération, le mécanisme de verrouillage de fichier ESX assure qu'aucun processus local n'accède au volume VMFS en conversion ; toutefois, vous devez vous assurer qu'aucun hôte ESX distant n'accède à ce volume. Cette conversion peut prendre plusieurs minutes. Une fois terminée, l'invite de commande s'affiche de nouveau.

A l'issue de la conversion, déchargez le pilote `fsaux` et chargez les pilotes `vmfs3` et `vmfs2` pour reprendre les opérations normales.

- `-u --upgradefinish`

  Cette option permet de terminer la mise à niveau.

Options de disque virtuel

Les options de disque virtuel permettent de configurer, migrer et gérer les disques virtuels stockés dans les systèmes de fichiers VMFS-2, VMFS-3 et NFS. Vous pouvez également exécuter un grand nombre de ces tâches via vSphere Client.

Formats de disque pris en charge

Lorsque vous créez ou clonez un disque virtuel, vous pouvez utiliser la sous-option `-d --diskformat` pour spécifier le format du disque.

Vous avez le choix entre les formats suivants :

- `zeroedthick` (valeur par défaut) – L'espace requis pour le disque virtuel est alloué au cours de la création. Toutes les données qui demeurent sur le périphérique physique ne sont pas effacées pendant la création, mais sont mises à zéro sur demande à la première écriture sur la machine virtuelle. La machine virtuelle ne lit pas les données caduques du disque.
- `eagerzeroedthick` – L'espace requis pour le disque virtuel est alloué pendant la création. Contrairement au format `zeroedthick`, les données qui demeurent sur le périphérique physique sont mises à zéro pendant la création. La création de disques à ce format peut être plus longue que pour d'autres types de disques.
- `thick` – L'espace requis pour le disque virtuel est alloué pendant la création. Ce type de formatage ne met pas à zéro les anciennes données qui se trouvent éventuelleemnt dans cet espace alloué. Seuls les utilisateur racine sont autorisés à effectuer des créations en utilisant ce format.
- `thin` – Disque virtuel léger. Contrairement au format `thick`, l'espace requis pour le disque virtuel n'est pas alloué pendant la création, mais il est fourni ultérieurement, sur demande.
- `rdm` – Mappage de disque brut en mode de compatibilité virtuelle.
- `rdmp` – Mappage de disque brut en mode de compatibilité physique (pass-through).
- `raw` – Périphérique brut.

- `2gbsparse` – Disque clairsemé possédant une taille d'extension maximale de 2 Go. Vous pouvez utiliser des disques de ce format avec d'autres produits VMware ; toutefois, vous ne pouvez pas utiliser de disques clairsemés sur un hôte ESX, sauf si vous avez préalablement réimporté le disque à l'aide de `vmkfstools` en utilisant un format compatible (`thick` ou `thin`, par exemple).
- `monosparse` – Disque clairsemé monolithique. Vous pouvez utiliser des disques de ce format avec d'autres produits VMware.
- `monoflat` – Disque plat monolithique. Vous pouvez utiliser des disques de ce format avec d'autres produits VMware.

Remarque Les seuls formats de disque pouvant être utilisés pour NFS sont les suivants : `thin`, `thick`, `zerodthick` et `2gbsparse`.

`Thick`, `zeroedthick` et `thin` reviennent généralement au même, car c'est le serveur NFS qui décide de la règle d'allocation, et non l'hôte ESX. Sur la plupart des serveurs NFS, la règle d'allocation par défaut est `thin`.

Création d'un disque virtuel

Pour créer un disque virtuel, utilisez la commande `vmkfstools`.

```
-c --createvirtualdisk size[kK|mM|gG]
      -a --adaptertype [buslogic|lsilogic] srcfile
      -d --diskformat [thin|zeroedthick|eagerzeroedthick]
```

Cette option permet de créer un disque virtuel à l'emplacement spécifié d'un volume VMFS. Spécifiez la taille du disque virtuel. Lorsque vous entrez la valeur du paramètre *size*, vous pouvez indiquer le type d'unité via l'ajout d'un suffixe `k` (kilo-octets), `m` (méga-octets) ou `g` (giga-octets). Le type d'unité ne respecte pas la casse. `vmkfstools` considère que `k` et `K` signifient kilo-octets. Si vous ne spécifiez aucun type d'unité, `vmkfstools` utilise par défaut les octets.

Vous pouvez spécifier les sous-options suivantes avec l'option `-c`.

- `-a` spécifie le pilote de périphérique utilisé pour communiquer avec les disques virtuels. Vous avez le choix entre des pilotes SCSI BusLogic et LSI Logic.
- `-d` permet de spécifier les formats de disque.

Exemple de création de disque virtuel

Cet exemple illustre la création d'un fichier de disque virtuel (d'une taille de deux giga-octets) appelé `rh6.2.vmdk` sur le système de fichiers VMFS `myVMFS`. Ce fichier représente un disque virtuel vide auquel les machines virtuelles peuvent accéder.

```
vmkfstools -c 2048m /vmfs/volumes/myVMFS/rh6.2.vmdk
```

Initialisation d'un disque virtuel

Pour initialiser un disque virtuel, utilisez la commande `vmkfstools`.

```
-w --writezeros
```

Cette option permet de nettoyer le disque virtuel en inscrivant des zéros sur toutes les données qu'il contient. En fonction de la taille de votre disque virtuel et de la bande passante d'E/S utilisée pour le périphérique hébergeant le disque virtuel, l'exécution de cette commande peut être plus ou moins longue.

Avertissement Lorsque vous utilisez cette commande, vous perdez les données présentes sur le disque virtuel.

Gonflage d'un disque virtuel léger

Pour gonfler un disque virtuel léger, utilisez la commande `vmkfstools`.

`-j --inflatedisk`

Cette option permet de convertir un disque virtuel léger (`thin`) en disque `eagerzeroedthick`, tout en préservant la totalité des données existantes. Cette option permet d'allouer les blocs qui ne l'ont pas encore été et de les mettre à zéro.

Suppression de blocs mis à zéro

Pour convertir des disques virtuels légers zeroedthick ou eagerzeroedthick en disques légers avec suppression des blocs mis à zéro, utilisez la commande `vmkfstools`.

`-K --punchzero`

Cette option permet de supprimer l'allocation de tous les blocs mis à zéro, en conservant uniquement ceux qui ont été alloués précédemment et qui contiennent des données. Le format du disque virtuel ainsi obtenu est le format de disque léger.

Conversion d'un disque virtuel Zeroedthick en disque Eagerzeroedthick

Pour convertir un disque virtuel zeroedthick en disque eagerzeroedthick, utilisez la commande `vmkfstools`.

`-k --eagerzero`

Outre la conversion, cette option permet de préserver les données présentes sur le disque virtuel.

Suppression d'un disque virtuel

Cette option permet de supprimer les fichiers associés au disque virtuel situé à l'emplacement spécifié du volume VMFS.

`-U --deletevirtualdisk`

Affectation d'un nouveau nom à un disque virtuel

Cette option permet de renommer un fichier associé au disque virtuel spécifié dans le chemin figurant dans la ligne de commande.

Vous devez spécifier le nom de fichier ou le chemin d'origine (*oldName*) et le nouveau nom de fichier ou le nouveau chemin (*newName*).

`-E --renamevirtualdisk` *`oldName newName`*

Clonage d'un disque virtuel ou d'un disque brut

Cette option permet de créer la copie d'un disque virtuel ou d'un disque brut spécifié.

```
-I --importfile srcfile -d --diskformat
   [rdm:device|rdmp:device|
      raw:device|thin|2gbsparse|monosparse|monoflat]
```

Vous pouvez utiliser la sous-option `-d` pour l 'option `-I`. Cette sous-option permet de spécifier le format de disque à utiliser pour la copie créée. Les utilisateurs autres que racine ne sont pas autorisés à effectuer le clonage de disques virtuels ou de disques bruts.

Remarque Pour cloner les fichiers redo-log ESX tout en conservant leur hiérarchie, utilisez la commande `cp`.

Exemple de clonage de disque virtuel

Cet exemple illustre le clonage du contenu d'un disque virtuel maître du référentiel `templates` vers un fichier de disque virtuel nommé `myOS.vmdk`, situé sur le système de fichiers `myVMFS`.

```
vmkfstools –I /vmfs/volumes/templates/gold–master.vmdk /vmfs/volumes/myVMFS/myOS.vmdk
```

Vous pouvez configurer une machine virtuelle en vue de l'utilisation de ce disque : pour cela, ajoutez les lignes correspondantes au fichier de configuration de la machine virtuelle, comme indiqué dans l'exemple suivant :

```
scsi0:0.present = TRUE
scsi0:0.fileName = /vmfs/volumes/myVMFS/myOS.vmdk
```

Migration de machines virtuelles VMware Workstation et VMware GSX Server

Vous ne pouvez pas utiliser vSphere Client pour migrer les machines virtuelles créées à l'aide de VMware Workstation ou VMware GSX Server au sein de votre système ESX. En revanche, vous pouvez utiliser la commande `vmkfstools –I` pour importer le disque virtuel sur votre système ESX, puis associer ce disque à une nouvelle machine virtuelle créée dans ESX.

Vous devez commencer par importer le disque virtuel, car vous ne pouvez pas utiliser les disques exportés au format `2gbsparse` sur un hôte ESX.

Procédure

1 Importez un disque Workstation ou GSX Server dans votre répertoire ou sous-répertoire `/vmfs/volumes/myVMFS/`.

2 Dans vSphere Client, créez une nouvelle machine virtuelle à l'aide de l'option de configuration **[Personnalisée]** .

3 Lorsque vous configurez un disque, sélectionnez **[Utiliser un disque virtuel existant]** , puis associez le disque Workstation ou GSX Server importé.

Extension d'un disque virtuel

Après la création d'une machine virtuelle, cette option permet d'en augmenter la taille.

```
–X ––extendvirtualdisk newSize[kK|mM|gG]
```

Avant d'entrer cette commande, vous devez mettre hors tension la machine virtuelle qui utilise ce fichier de disque. Vous devrez peut-être mettre à niveau le système de fichiers du disque, afin que le système d'exploitation invité puisse reconnaître et utiliser la nouvelle taille de disque (et donc l'espace disponible supplémentaire).

Vous pouvez spécifier la valeur du paramètre `newSize` en kilo-octets, en méga-octets ou en giga-octets : pour cela, ajoutez un suffixe `k` (kilo-octets), `m` (méga-octets) ou `g` (giga-octets). Le type d'unité ne respecte pas la casse. `vmkfstools` considère que `k` et `K` signifient kilo-octets. Si vous ne spécifiez aucun type d'unité, `vmkfstools` utilise par défaut les kilo-octets.

Le paramètre `newSize` définit la nouvelle taille totale (et pas uniquement l'incrément ajouté au disque).

Par exemple, pour étendre un disque virtuel de 4 Go d'1 Go, entrez : **`vmkfstools –X 5g disk name.dsk`**

Remarque N'étendez pas le disque de base d'une machine virtuelle associée à des snapshots. En effet, cela vous empêcherait de valider les snapshots ou de restaurer la taille d'origine du disque de base.

Migration d'un disque virtuel VMFS-2 vers un disque VMFS-3

Cette option permet de convertir le fichier de disque virtuel spécifié du format ESX Server 2 vers le format ESX.

`-M --migratevirtualdisk`

Création d'un mappage de périphérique brut en mode de compatibilité virtuelle

Cette option permet de créer un fichier de mappage de périphérique brut (RDM) sur un volume VMFS-3, et de mapper un disque brut sur ce fichier. Une fois ce mappage établi, vous pouvez accéder au disque brut comme vous le feriez pour un disque virtuel VMFS classique. La longueur du fichier objet du mappage est équivalente à la taille du disque brut désigné.

`-r --createrdm` *`device`*

Lorsque vous spécifiez la valeur du paramètre *device*, respectez le format suivant :

`/vmfs/devices/disks/vml.`*`vml_ID`*

REMARQUE Les 3 mécanismes de verrouillage de fichier VMFS s'appliquent aux RDM.

Exemple de création d'un fichier RDM en mode de compatibilité virtuelle

Dans cet exemple, vous créez un fichier RDM appelé `my_rdm.vmdk` et vous mappez le disque brut `vml.`*`vml_ID`* sur ce fichier.

`vmkfstools -r /vmfs/devices/disks/vml.`*`vml_ID`* `my_rdm.vmdk`

Vous pouvez configurer une machine virtuelle en vue de l'utilisation du fichier de mappage `my_rdm.vmdk` ; pour cela, ajoutez les lignes suivantes au fichier de configuration de la machine virtuelle :

```
scsi0:0.present = TRUE
scsi0:0.fileName = /vmfs/volumes/myVMFS/my_rdm.vmdk
```

Création d'un mappage de périphérique brut en mode de compatibilité physique

Cette option permet de mapper un périphérique brut d'émulation sur un fichier de volume VMFS. Ce mappage permet à une machine virtuelle d'ignorer le filtrage de commandes SCSI ESX lors de l'accès au disque virtuel. Ce type de mappage est très utile lorsque la machine virtuelle doit envoyer des commandes SCSI prioritaires (par exemple, lorsqu'un logiciel compatible SAN est exécuté sur la machine virtuelle).

`-z --createrdmpassthru` *`device`*

Une fois ce type de mappage établi, vous pouvez l'utiliser pour l'accès au disque brut, comme vous le feriez pour les autres disques virtuels VMFS.

Lorsque vous spécifiez la valeur du paramètre *device*, respectez le format suivant :

`/vmfs/devices/disks/vml.`*`vml_ID`*

Liste des attributs d'un RDM

Cette option permet de répertorier les attributs d'un mappage de disque brut.

`-q --queryrdm`

Cette option imprime le nom du RDM du disque brut. Elle imprime également d'autres informations d'identification (ID de disque du disque brut, par exemple).

Affichage de la géométrie de disque virtuel

Cette option permet d'obtenir des informations sur la géométrie d'un disque virtuel.

`-g --geometry`

Le résultat se présente comme suit : `Geometry information C/H/S`, où `C` représente le nombre de cylindres, `H` représente le nombre de têtes et `S` représente le nombre de secteurs.

Remarque Lorsque vous importez des disques virtuels VMware Workstation sur un hôte ESX, un message d'erreur s'affiche : il indique une divergence de géométrie de disque. Les divergences de géométrie de disque peuvent également être à l'origine de problèmes de chargement d'un système d'exploitation invité ou d'exécution d'une machine virtuelle créée.

Vérification et réparation des disques virtuels

Utilisez cette option pour vérifier ou réparer un disque virtuel en cas d'arrêt anormal.

`-x , -fix [check|repair]`

Gestion des réservations SCSI de LUN

L'option `-L` permet d'exécuter des tâches administratives pour les périphériques de stockage physiques. Vous pouvez exécuter un grand nombre de ces tâches via vSphere Client.

`-L --lock [reserve|release|lunreset|targetreset|busreset]`*`device`*

Cette option vous permet de réserver un LUN SCSI à des fins d'utilisation exclusive par un hôte ESX, de libérer une réservation pour que d'autres hôtes puissent accéder au LUN, ou encore de rétablir une réservation forçant la libération de toutes les réservations de la cible.

Avertissement L'utilisation de l'option `-L` peut interrompre les opérations des autres serveurs d'un SAN. Veillez à utiliser l'option `-L` uniquement pour le dépannage de configurations de clusters.

Sauf recommandation contraire de VMware, n'utilisez jamais cette option sur un volume LUN hébergeant un volume VMFS.

Vous pouvez spécifier l'option `-L` de différentes façons :

- `-L reserve` – Permet de réserver le LUN spécifié. Une fois la réservation effectuée, seul le serveur ayant réservé ce LUN peut y accéder. Si d'autres serveurs tentent d'accéder à ce LUN, un message d'erreur de réservation s'affiche.
- `-L release` – Permet de libérer la réservation du LUN spécifié. Dans ce cas, les autres serveurs peuvent de nouveau y accéder.
- `-L lunreset` – Permet de restaurer le LUN spécifié via la suppression des réservations associées ; le LUN redevient disponible pour tous les autres serveurs. Cette restauration n'affecte pas les autres LUN du périphérique. Si l'un d'entre eux est réservé, il le reste.
- `-L targetreset` – Permet de restaurer la cible complète. Cette opération supprime les réservations de tous les LUN associés à cette cible ; ces LUN redeviennent disponibles pour tous les serveurs.
- `-L busreset` – Permet de restaurer toutes les cibles accessibles sur le bus. Cette opération supprime les réservations de tous les LUN accessibles via le bus, et les rend de nouveau disponibles pour tous les serveurs.

Lorsque vous entrez la valeur du paramètre *device*, respectez le format suivant :

`/vmfs/devices/disks/vml.`*`vml_ID`*`:P`

Index

B

C

D

E

F

G

L

M

N

R

S

W