

# Gestion des hôtes uniques vSphere - VMware Host Client

VMware vSphere 8.0

VMware ESXi 8.0

VMware Host Client 2.5.0

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

<https://docs.vmware.com/fr/>

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

**VMware France SAS.**  
Tour Franklin  
100-101 Terrasse Boieldieu  
92042 Paris La Défense 8 Cedex  
France  
[www.vmware.com/fr](http://www.vmware.com/fr)

Copyright © 2015-2022 VMware, Inc. Tous droits réservés. [Informations relatives aux copyrights et marques commerciales.](#)

# Table des matières

À propos de Gestion individuelle des hôtes vSphere - VMware Host Client 9

## 1 Informations mises à jour 10

## 2 Qu'est-ce que VMware Host Client 11

Utiliser la VMware Host Client. 12

Démarrer VMware Host Client et se connecter 12

Se déconnecter de VMware Host Client 12

Personnalisation de votre thème d'interface utilisateur VMware Host Client 12

Configurer une bannière de connexion pour l'écran de connexion de l'interface utilisateur de VMware Host Client 15

Quitter ou rejoindre le programme d'amélioration du produit dans VMware Host Client 19

## 3 Gestion des hôtes avec VMware Host Client 21

Gérer les paramètres système dans VMware Host Client 21

Gérer les paramètres avancés dans VMware Host Client 22

Créer un message de bienvenue initial pour l'interface utilisateur de la console directe (DCUI) et VMware Host Client 22

Configurer le délai d'expiration de session de l'interface utilisateur VMware Host Client 23

Configurer le délai d'expiration de session SOAP dans VMware Host Client 24

Configurer la politique de mot de passe et de verrouillage de compte dans VMware Host Client 25

Configurer Syslog dans VMware Host Client 29

Configurer les options de clé TLS/SSL avancées 30

Configurer la mise à zéro de la mémoire userworld 32

Modifier la configuration du démarrage automatique dans VMware Host Client 33

Modifier la configuration de l'heure d'un hôte ESXi dans VMware Host Client 34

Gérer le matériel d'un hôte ESXi avec VMware Host Client 35

Règles de gestion de l'alimentation de l'hôte 35

Modifier les stratégies de gestion de l'alimentation dans VMware Host Client 36

Changer l'étiquette de matériel dans VMware Host Client 37

Attribution de licences pour les hôtes ESXi 37

Afficher les informations relatives aux licences de l'environnement VMware Host Client 39

Attribuer une clé de licence à un hôte ESXi dans VMware Host Client 39

Supprimer une licence d'un hôte ESXi dans VMware Host Client 39

Gérer les services dans VMware Host Client 40

Gestion de la sécurité et des utilisateurs pour un hôte ESXi avec VMware Host Client 40

Gérer l'authentification des hôtes avec VMware Host Client 41

Gérer les certificats des hôtes avec VMware Host Client 43

|  |    |
|--|----|
| Gérer les utilisateurs avec VMware Host Client   | 44 |
| Gérer les rôles ESXi dans VMware Host Client   | 46 |
| Gérer des hôtes dans vCenter Server  | 48 |
| Mettre à jour votre environnement VMware Host Client vers la dernière version  | 48 |
| Impossible de se connecter depuis VMware Host Client à un hôte ESXi après la mise à niveau vers une version plus récente de ESXi | 49 |
| Accéder à vSphere Client   | 50 |
| Déconnecter un hôte ESXi de vCenter Server avec VMware Host Client   | 51 |
| Redémarrer ou arrêter ESXi Host dans VMware Host Client  | 51 |
| Utilisation du ESXi Shell  | 52 |
| Activer Secure Shell (SSH) dans VMware Host Client   | 52 |
| Activer ESXi Console Shell dans VMware Host Client   | 53 |
| Créer un délai d'expiration pour la disponibilité d'ESXi Shell dans VMware Host Client   | 53 |
| Créer un délai d'expiration pour les sessions ESXi Shell inactives dans VMware Host Client                                       | 54 |
| Mettre un hôte en mode de maintenance dans VMware Host Client  | 55 |
| Gérer les autorisations dans VMware Host Client  | 55 |
| Validation d'autorisation  | 56 |
| Attribuer des autorisations à un utilisateur pour un hôte ESXi dans VMware Host Client   | 57 |
| Supprimer des autorisations pour un utilisateur dans VMware Host Client  | 57 |
| Attribuer des autorisations utilisateur pour une machine virtuelle dans VMware Host Client                                       | 58 |
| Supprimer des autorisations pour une machine virtuelle dans VMware Host Client   | 58 |
| Générer un bundle de support dans VMware Host Client   | 59 |
| Mode de verrouillage dans VMware Host Client   | 59 |
| Mettre un hôte ESXi en mode de verrouillage normal avec VMware Host Client   | 60 |
| Mettre un hôte ESXi en mode de verrouillage strict avec VMware Host Client   | 60 |
| Quitter le mode de verrouillage avec VMware Host Client  | 61 |
| Spécifier les utilisateurs exceptionnels du mode de verrouillage dans VMware Host Client   | 61 |
| Gérer des ressources CPU à l'aide de VMware Host Client  | 61 |
| Afficher les informations sur les processeurs en utilisant VMware Host Client  | 62 |
| Attribuer une machine virtuelle à un processeur spécifique dans VMware Host Client   | 62 |
| Surveiller un hôte ESXi dans VMware Host Client  | 62 |
| Afficher les graphiques dans VMware Host Client  | 62 |
| Surveiller l'état de santé du matériel dans VMware Host Client   | 63 |
| Afficher les événements dans VMware Host Client  | 63 |
| Afficher les tâches dans VMware Host Client  | 64 |
| Afficher les journaux système dans VMware Host Client  | 64 |
| Afficher les notifications dans VMware Host Client   | 64 |

## 4 Gestion des machines virtuelles avec VMware Host Client 66

|   |    |
|---|----|
| Créer une machine virtuelle dans VMware Host Client | 66 |
|---|----|

|  |     |
|--|-----|
| Enregistrer une machine virtuelle existante dans VMware Host Client                                | 71  |
| Utiliser les consoles dans VMware Host Client  | 72  |
| Installer l'application VMware Remote Console dans VMware Host Client                              | 72  |
| Lancer la console distante pour une machine virtuelle dans VMware Host Client                      | 73  |
| Ouvrir une console de machine virtuelle dans VMware Host Client                                    | 73  |
| Gérer un système d'exploitation invité dans VMware Host Client                                     | 74  |
| Arrêter et redémarrer un système d'exploitation invité en utilisant VMware Host Client             | 74  |
| Changer le système d'exploitation invité dans VMware Host Client                                   | 74  |
| Présentation de VMware Tools   | 75  |
| Installation de VMware Tools   | 76  |
| Installer VMware Tools à partir d'VMware Host Client   | 76  |
| Mise à niveau de VMware Tools  | 76  |
| Mise à niveau de VMware Tools dans VMware Host Client  | 78  |
| Configuration d'une machine virtuelle dans VMware Host Client                                      | 79  |
| Vérifier la version matérielle d'une machine virtuelle dans VMware Host Client                     | 79  |
| Modifier le nom d'une machine virtuelle dans VMware Host Client                                    | 79  |
| Afficher l'emplacement du fichier de configuration des machines virtuelles dans VMware Host Client | 80  |
| Configurer les états d'alimentation de la machine virtuelle dans VMware Host Client                | 80  |
| Modifier les paramètres des fichiers de configuration dans VMware Host Client                      | 82  |
| Configurer le démarrage automatique pour une machine virtuelle dans VMware Host Client             | 83  |
| Mettre à niveau la compatibilité des machines virtuelles à l'aide de VMware Host Client            | 84  |
| Gérer des machines virtuelles dans VMware Host Client  | 85  |
| Accès à une machine virtuelle dans VMware Host Client  | 85  |
| États d'alimentation d'une machine virtuelle dans VMware Host Client                               | 85  |
| Utiliser la configuration des colonnes des machines virtuelles dans VMware Host Client             | 86  |
| Supprimer des machines virtuelles d'un hôte dans VMware Host Client                                | 87  |
| Supprimer des machines virtuelles de la banque de données dans VMware Host Client                  | 87  |
| Enregistrer une machine virtuelle dans VMware Host Client  | 87  |
| Gérer des machines virtuelles avec des snapshots   | 88  |
| Fichiers de snapshot   | 90  |
| Limitations des snapshots  | 91  |
| Créer un snapshot d'une machine virtuelle dans VMware Host Client                                  | 92  |
| Restaurer le snapshot le plus récent dans VMware Host Client                                       | 94  |
| Supprimer un snapshot dans VMware Host Client  | 96  |
| Suppression des snapshots  | 97  |
| Pourquoi utiliser le gestionnaire de snapshots dans VMware Host Client                             | 99  |
| Surveiller une machine virtuelle dans VMware Host Client   | 99  |
| Afficher les graphiques de performances des machines virtuelles dans VMware Host Client            | 99  |
| Afficher les événements des machines virtuelles dans VMware Host Client                            | 100 |

|   |     |
|---|-----|
| Afficher les tâches des machines virtuelles dans VMware Host Client               | 100 |
| Afficher l'explorateur de journaux de machines virtuelles dans VMware Host Client | 101 |
| Afficher les notifications des machines virtuelles dans VMware Host Client        | 101 |

## 5 Configurer le matériel d'une machine virtuelle dans VMware Host Client 102

|  |     |
|--|-----|
| Configuration de CPU virtuel   | 102 |
| Limitations du CPU virtuel   | 103 |
| Configuration de CPU multicœurs virtuelles   | 104 |
| Changer le nombre de CPU virtuels  | 104 |
| Allouer des ressources CPU dans VMware Host Client   | 105 |
| Configuration de la mémoire virtuelle  | 106 |
| Changer la configuration de mémoire  | 107 |
| Allouer les ressources en mémoire  | 108 |
| Changer les paramètres d'ajout de mémoire à chaud  | 109 |
| Ajout d'un périphérique NVDIMM à une machine virtuelle dans VMware Host Client                           | 110 |
| Configuration de la machine virtuelle de réseau  | 111 |
| Notions de base des adaptateurs réseau   | 111 |
| Adaptateurs réseau et machines virtuelles héritées   | 114 |
| Modifier la configuration de l'adaptateur réseau virtuel dans VMware Host Client                         | 114 |
| Ajouter une carte réseau à une machine virtuelle dans VMware Host Client                                 | 115 |
| Configuration de disque virtuel  | 115 |
| À propos des règles de provisionnement des disques virtuels  | 116 |
| Changer la configuration d'un disque virtuel dans VMware Host Client                                     | 117 |
| Ajouter un nouveau disque dur standard à une machine virtuelle dans VMware Host Client                   | 118 |
| Ajouter un disque dur existant à une machine virtuelle dans VMware Host Client                           | 121 |
| Ajouter un disque à mémoire persistante dans Host Client   | 122 |
| Utiliser les partages de disque pour définir la priorité des machines virtuelles dans VMware Host Client | 124 |
| Configuration des contrôleurs de machines virtuelles dans VMware Host Client                             | 124 |
| Ajouter un contrôleur USB à une machine virtuelle  | 125 |
| Ajouter des contrôleurs SCSI dans VMware Host Client   | 126 |
| Changer la configuration du partage de bus SCSI dans VMware Host Client                                  | 127 |
| Changer le type de contrôleur SCSI dans VMware Host Client   | 127 |
| À propos des contrôleurs SCSI paravirtuels VMware  | 128 |
| Ajouter un contrôleur Paravirtual SCSI dans VMware Host Client   | 129 |
| Ajouter un contrôleur SATA à une machine virtuelle dans VMware Host Client                               | 129 |
| Ajouter un contrôleur NVMe dans VMware Host Client   | 130 |
| Autre configuration de périphérique de machine virtuelle dans VMware Host Client                         | 131 |
| Ajouter un lecteur de CD-ROM ou de DVD-ROM à une machine virtuelle dans VMware Host Client               | 131 |
| Ajouter un lecteur de disquette à une machine virtuelle dans VMware Host Client                          | 132 |

|   |     |
|---|-----|
| Ajouter un périphérique USB à une machine virtuelle dans VMware Host Client   | 133 |
| Ajouter un contrôleur audio à une machine virtuelle dans VMware Host Client   | 134 |
| Configuration de ports parallèles et de ports série dans VMware Host Client   | 134 |
| Utilisation d'un temporisateur de surveillance virtuel  | 136 |
| Ajouter un périphérique horloge de précision à une machine virtuelle dans VMware Host Client                                    | 138 |
| Ajouter un périphérique PCI à une machine virtuelle dans VMware Host Client   | 138 |
| Sécurisation des machines virtuelles dans VMware Host Client  | 139 |
| Activer vSGX sur une machine virtuelle dans VMware Host Client  | 140 |
| Désactiver vSGX sur une machine virtuelle dans VMware Host Client   | 141 |
| Supprimer un périphérique vTPM d'une machine virtuelle dans VMware Host Client  | 141 |
| Activer ou désactiver la sécurité basée sur la virtualisation (VBS) sur une machine virtuelle existante dans VMware Host Client | 142 |

## 6 Gestion du stockage dans VMware Host Client 145

|  |     |
|--|-----|
| Banques de données dans VMware Host Client   | 145 |
| Afficher les informations sur les banques de données dans VMware Host Client                   | 146 |
| Créer une banque de données VMFS dans VMware Host Client                                       | 146 |
| Augmentation de la capacité d'une banque de données VMFS                                       | 147 |
| Montage d'une banque de données NFS (Network File System) dans VMware Host Client              | 149 |
| Démonter une banque de données dans VMware Host Client   | 150 |
| Utilisation de l'explorateur de fichiers de banques de données dans VMware Host Client         | 151 |
| Renommer une banque de données dans VMware Host Client   | 155 |
| Supprimer une banque de données VMFS dans VMware Host Client                                   | 156 |
| Provisionnement dynamique du stockage dans VMware Host Client                                  | 156 |
| Gestion des adaptateurs de stockage dans VMware Host Client                                    | 158 |
| Afficher les adaptateurs de stockage dans VMware Host Client                                   | 158 |
| Configuration d'adaptateurs iSCSI logiciels dans VMware Host Client                            | 158 |
| Gestion des périphériques de stockage dans VMware Host Client                                  | 169 |
| Afficher les périphériques de stockage dans VMware Host Client                                 | 169 |
| Effacer une table de partition de périphérique dans VMware Host Client                         | 169 |
| Modifier individuellement des partitions de périphériques dans VMware Host Client              | 169 |
| Gestion de la mémoire persistante  | 170 |
| Modes de consommation des ressources de mémoire persistante de l'hôte                          | 170 |
| Structure de la banque de données PMem   | 172 |
| Surveillance du stockage dans VMware Host Client   | 174 |
| Surveiller les banques de données dans VMware Host Client                                      | 174 |
| Surveillance de vSAN dans VMware Host Client   | 175 |
| Effectuer une actualisation du stockage et des opérations de réanalyse dans VMware Host Client | 180 |
| Exécution d'une réanalyse des adaptateurs dans VMware Host Client                              | 180 |
| Exécution d'une réanalyse de périphériques dans VMware Host Client                             | 180 |

Modifier le nombre de périphériques de stockage analysés dans VMware Host Client 181

## 7 Mise en réseau dans VMware Host Client 182

Gérer les groupes de ports dans VMware Host Client 182

Afficher les informations sur les groupes de ports dans VMware Host Client 182

Ajouter un groupe de ports de commutateur virtuel dans VMware Host Client 183

Modifier les paramètres des groupes de ports dans VMware Host Client 183

Supprimer un groupe de ports de commutateur virtuel dans VMware Host Client 188

Gérer des commutateurs virtuels dans VMware Host Client 188

Afficher les informations sur les commutateurs virtuels dans VMware Host Client 189

Ajouter un commutateur virtuel standard dans VMware Host Client 189

Supprimer un commutateur virtuel dans VMware Host Client 190

Ajouter une liaison montante physique à un commutateur virtuel dans VMware Host Client 191

Modifier les paramètres des commutateurs virtuels dans VMware Host Client 191

Gérer les adaptateurs réseau physiques dans VMware Host Client 196

Afficher les informations sur les cartes réseau physiques dans VMware Host Client 196

Modifier les cartes réseau physiques dans VMware Host Client 196

Gérer des adaptateurs réseau VMkernel dans VMware Host Client 196

Afficher les informations sur l'adaptateur réseau VMkernel dans VMware Host Client 196

Ajouter un adaptateur réseau VMkernel dans VMware Host Client 197

Modifier les paramètres des adaptateurs réseau VMkernel dans VMware Host Client 198

Supprimer un adaptateur réseau VMkernel dans VMware Host Client 199

Afficher la configuration des piles TCP/IP sur un hôte dans VMware Host Client 200

Modifier la configuration d'une pile TCP/IP sur un hôte dans VMware Host Client 200

Configurer le pare-feu ESXi dans VMware Host Client 201

Gérer les paramètres du pare-feu ESXi à l'aide de VMware Host Client 202

Ajouter des adresses IP autorisées pour ESXi Host avec VMware Host Client 202

Surveiller des événements et tâches de mise en réseau dans VMware Host Client 203

Surveiller les groupes de ports dans VMware Host Client 203

Surveiller les commutateurs virtuels dans VMware Host Client 203

Surveiller des adaptateurs réseau physiques dans VMware Host Client 204

Surveiller des adaptateurs réseau VMkernel dans VMware Host Client 204

Surveiller les piles TCP/IP dans VMware Host Client 204



# À propos de Gestion individuelle des hôtes vSphere - VMware Host Client

Le document *vSphere Single Host Management - VMware Host Client* fournit des informations sur la gestion individuelle des hôtes avec VMware Host Client.

VMware Host Client peut être utilisé pour effectuer la gestion des urgences si vCenter Server est indisponible. Vous pouvez utiliser VMware Host Client pour effectuer des tâches administratives, de dépannage de base et des tâches administratives avancées.

VMware prend l'intégration au sérieux. Pour encourager ce principe auprès de nos clients, nos partenaires et notre communauté interne, nous avons mis à jour ce guide pour supprimer des éléments de langage ne respectant pas le principe de l'intégration.

## Public cible

Ces informations sont destinées à toutes les personnes qui souhaitent utiliser VMware Host Client pour gérer individuellement les hôtes ESXi. Elles sont destinées aux administrateurs Windows ou Linux expérimentés qui maîtrisent les technologies de machine virtuelle et les opérations de centre de données.

# Informations mises à jour

# 1

La documentation relative à la *Gestion individuelle des hôtes vSphere - VMware Host Client* est mise à jour avec chaque nouvelle version du produit ou lorsque cela s'avère nécessaire.

Ce tableau affiche l'historique des mises à jour du *Gestion individuelle des hôtes vSphere - VMware Host Client*.

| Révision        | Description   |
|-----------------|---|
| 21 octobre 2022 | Mises à jour mineures de <a href="#">Gérer les paramètres système</a> dans VMware Host Client.  |
| 19 octobre 2022 | Mises à jour mineures de <a href="#">Activer ou désactiver la sécurité basée sur la virtualisation (VBS)</a> sur une machine virtuelle existante dans VMware Host Client.                                   |
| 13 octobre 2022 | Suppression des espaces vides dans les extraits de code de <a href="#">Impossible de se connecter depuis VMware Host Client à un hôte ESXi après la mise à niveau vers une version plus récente de ESXi</a> |
| 11 octobre 2022 | Version initiale.   |

# Qu'est-ce que VMware Host Client

## 2

VMware Host Client est un client basé sur HTML 5 qui permet de se connecter à des hôtes ESXi et de gérer chaque hôte individuellement.

Vous pouvez utiliser VMware Host Client pour :

- Effectuer des tâches administratives et de dépannage de base ainsi que des tâches administratives avancées sur votre hôte ESXi cible.
- Effectuer une gestion des urgences lorsque vCenter Server n'est pas disponible.

Il est important de savoir que l'instance de VMware Host Client est différente de l'instance de vSphere Client. Utilisez vSphere Client pour vous connecter à vCenter Server et gérer plusieurs hôtes ESXi, et utilisez VMware Host Client pour gérer un hôte ESXi unique.

Les fonctions de VMware Host Client comprennent, sans s'y limiter, les opérations suivantes :

- Opérations de virtualisation de base, comme le déploiement et la configuration des machines virtuelles de complexité variable.
- Création et gestion de la mise en réseau et des banques de données
- Réglage avancé des options de niveau d'hôte pour améliorer les performances

## Configuration système requise pour VMware Host Client

Assurez-vous que votre navigateur prend en charge VMware Host Client.

VMware Host Client prend en charge les systèmes d'exploitation invités et les versions de navigateur Web suivants.

| Navigateurs pris en charge | Mac OS | Windows 32 bits et 64 bits | Linux |
|----------------------------|--------|----------------------------|-------|
| Google Chrome              | 89+    | 89+                        | 75+   |
| Mozilla Firefox            | 80+    | 80+                        | 60+   |
| Microsoft Edge             | 90+    | 90+                        | S.O.  |
| Safari                     | 9.0+   | S.O.                       | S.O.  |

Ce chapitre contient les rubriques suivantes :

- [Utiliser la VMware Host Client.](#)

## Utiliser la VMware Host Client.

Vous pouvez utiliser VMware Host Client pour effectuer une gestion des urgences quand vCenter Server est temporairement indisponible.

### Démarrer VMware Host Client et se connecter

Vous pouvez utiliser VMware Host Client pour gérer individuellement des hôtes ESXi et effectuer différentes tâches administratives et de dépannage sur vos machines virtuelles.

Pour vous connecter à l'hôte ESXi, procédez comme suit.

#### Procédure

- 1 Dans un navigateur Web, entrez le nom d'hôte ou l'adresse IP de la cible à l'aide du formulaire **`https://host-name/ui`** ou **`https://host-IP-address/ui`**.

Un écran de connexion apparaît.

- 2 Entrez votre nom d'utilisateur et votre mot de passe.
- 3 Cliquez sur **Connexion** pour continuer.
- 4 Passez en revue la page du programme d'amélioration du produit (CEIP) et indiquez si vous souhaitez rejoindre le programme.

Pour en savoir plus sur le programme et découvrir comment le configurer à tout moment, reportez-vous à [Quitter ou rejoindre le programme d'amélioration du produit dans VMware Host Client](#).

- 5 Cliquez sur **OK**.

### Se déconnecter de VMware Host Client

Lorsque vous n'avez plus besoin d'afficher ou de gérer votre hôte ESXi cible, déconnectez-vous de VMware Host Client.

---

**Note** La fermeture d'une session VMware Host Client n'arrête pas l'hôte.

---

#### Procédure

- ◆ Pour se déconnecter de l'hôte ESXi, cliquez sur le nom de l'utilisateur en haut de la fenêtre VMware Host Client et sélectionnez **Se déconnecter** dans le menu déroulant.

Vous êtes maintenant déconnecté de VMware Host Client. Votre hôte ESXi cible continue à exécuter toutes ses activités habituelles.

### Personnalisation de votre thème d'interface utilisateur VMware Host Client

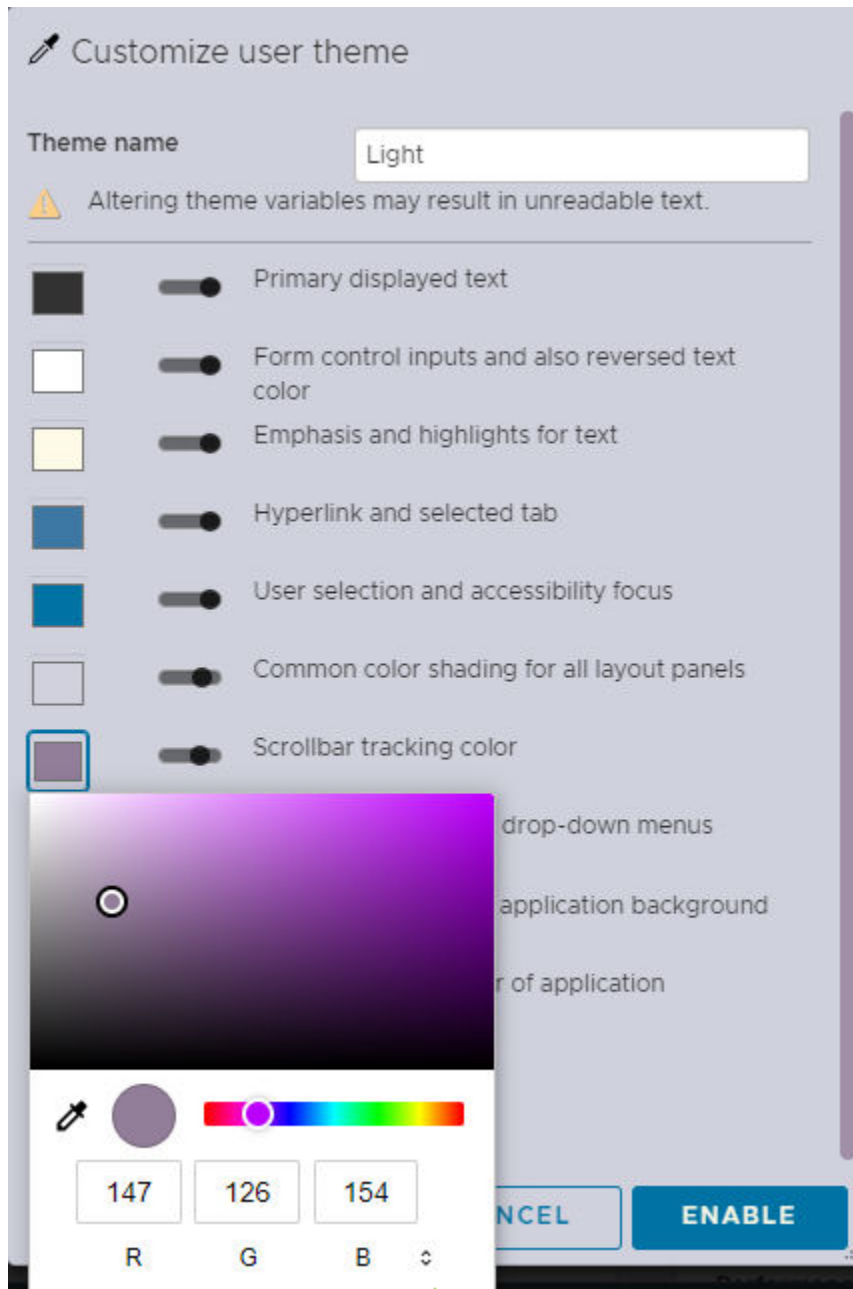
Avec vSphere 8.0, vous pouvez personnaliser les informations de marque de l'interface utilisateur de VMware Host Client et son apparence, ainsi que l'affichage du contenu.

Vous pouvez choisir parmi trois thèmes prédéfinis (clair, sombre et classique) et appliquer un thème à VMware Host Client selon vos préférences.

#### Procédure

- 1 Dans la barre d'outils VMware Host Client, cliquez sur **Aide**, puis sur **À propos de**.  
La fenêtre **À propos de** s'ouvre.
- 2 Dans le menu déroulant **Thème des préférences de l'UI**, sélectionnez le thème que vous souhaitez appliquer.

- 3 Pour changer le nom du thème et modifier jusqu'à 10 paramètres du thème que vous sélectionnez, cliquez sur le bouton **Personnaliser**.



- a Dans le champ **Nom du thème**, entrez un nom personnalisé pour le thème.
- b Pour sélectionner une couleur personnalisée pour chaque paramètre, cliquez sur la zone colorée devant chaque paramètre, sélectionnez une couleur, puis cliquez sur **Activer**.
- a Pour restaurer la palette par défaut, cliquez sur le bouton **Réinitialiser**.

## Configurer une bannière de connexion pour l'écran de connexion de l'interface utilisateur de VMware Host Client

Pour afficher des avertissements juridiques ou des annonces officielles, vous pouvez configurer une bannière de page de connexion en utilisant une forme limitée de syntaxe Markdown.

En modifiant le fichier texte `/etc/vmware/welcome` directement sur l'hôte, vous pouvez modifier le contenu de la bannière de connexion qui s'affiche à droite des champs de connexion du nom d'utilisateur et du mot de passe.

**Note** Un analyseur Markdown est appliqué au bloc de contenu et certaines séquences de caractères, telles que `#`, ```, `*`, peuvent déclencher involontairement des règles de formatage Markdown.

Vous pouvez appliquer l'ensemble limité suivant de directives Markdown dans le fichier `welcome`.

| Concept de disposition   | Syntaxe du code Markdown   | Sortie  |
|--------------------------|--|---|
| Étiquettes d'en-tête     | <ul style="list-style-type: none"> <li>■ À partir d'une nouvelle ligne, entrez entre 1 et 6 symboles de marque de hachage.</li> </ul> <p><b>Exemple</b></p> <pre># My Title.</pre>   | <p>Génère une grande balise HTML <code>&lt;h1&gt;</code> pour « Mon titre ».</p> <p><b>My Title</b></p>   |
| Règle horizontale        | <ul style="list-style-type: none"> <li>■ À partir d'une nouvelle ligne, entrez une série d'au moins 3 tirets uniquement.</li> </ul> <p><b>Exemple</b></p> <pre>-----.</pre>  | <p>Génère une balise de règle <code>&lt;hr /&gt;</code> au format HTML.</p> <hr/>   |
| Bloc littéral ou de code | <ul style="list-style-type: none"> <li>■ À partir d'une nouvelle ligne, entrez 3 apostrophes inversées (<code>'</code>) uniquement.</li> <li>■ Ajoutez le matériel source sur les lignes suivantes.</li> <li>■ Pour fermer la source, sur une nouvelle ligne, entrez 3 apostrophes inversées (<code>'</code>).</li> </ul> <p><b>Exemple</b></p> <pre>''' My content - - - *Login Secure* &gt;_ Read the policy '''</pre> | <p>Affiche le bloc de texte entre les lignes d'apostrophes inversées (<code>'</code>) sans formatage ni interprétation dans une police monospace.</p> <pre>My content - - - *Login Secure* &gt;_ Read the policy</pre> <p><b>Note</b> Si le contenu est accidentellement formaté par l'analyseur Markdown, encapsulez le contenu avec deux lignes de caractères d'apostrophes inversées. Étant donné que les caractères d'espace sont conservés, il est possible d'utiliser l'art ASCII, car la police est à espacement unique.</p> |
| Texte en gras            | <p>Encadrez une chaîne de texte par deux astérisques de chaque côté.</p> <p><b>Exemple</b></p> <pre>**important message**.</pre> <p><b>Note</b> La syntaxe Markdown des caractères de soulignement doubles est omise afin d'éviter tout conflit avec les URL.</p>  | <p><b>&lt;b&gt;message important&lt;/b&gt;</b></p>  |

| Concept de disposition | Syntaxe du code Markdown  | Sortie   |
|------------------------|---|--|
| Texte en italique      | <p>Encapsuler une chaîne de texte avec un seul astérisque des deux côtés.</p> <p><b>Exemple</b></p> <pre>*A named document*.</pre> <hr/> <p><b>Note</b> La syntaxe des caractères de soulignement Markdown est omise afin d'éviter tout conflit avec les URL.</p> | <pre>&lt;i&gt;Un document nommé&lt;/i&gt;</pre>  |
| Lien hypertexte        | <p>Pour lier une URL absolue, utilisez la syntaxe Markdown des crochets autour du texte du lien, suivis de parenthèses encadrant l'URL.</p> <p><b>Exemple</b></p> <pre>[My link] (https://www.example.com?search=virtual)</pre>                                   | <p>Génère une balise d'ancrage de lien hypertexte normale avec du texte sur lequel il est possible de cliquer.</p> <pre>&lt;a href="https://www.example.com?search=virtual"&gt;My link&lt;/a&gt;</pre> |

## Variables prises en charge

Vous pouvez insérer les variables suivantes n'importe où dans le fichier texte.

| Concept de variable  | Code de variable de balise méta | Sortie  |
|--|---------------------------------|---|
| Nom de domaine complet de l'hôte ou de l'adresse IP actuel           | {hostname}                      | Affiche le nom complet de l'hôte actuel. Par exemple, sample.host.com   |
| Version d'ESXi sous forme de format numérique à séparation par point | {esxversion}                    | Affiche, par exemple, 7.0.0   |
| Nom de produit complet d'ESXi, version et numéro de build            | {esxproduct}                    | Affiche, par exemple, VMware ESXi 7.0.0 build-16324942  |
| Date actuelle de la machine de l'utilisateur                         | {client-current-date}           | <p>Affiche, par exemple, Tuesday, August 30, 2022</p> <hr/> <p><b>Note</b> Cela est spécifique aux paramètres régionaux</p> |
| Heure actuelle sur la machine de l'utilisateur                       | {client-current-time}           | <p>Affiche, par exemple, 08:00 AM</p> <hr/> <p><b>Note</b> Cela est spécifique aux paramètres régionaux</p>                 |

## Balises avancées

Les balises avancées offrent des changements visuels et comportementaux en fonction des règles que vous appliquez à la page de connexion. Insérez ces balises à la toute fin du fichier texte.



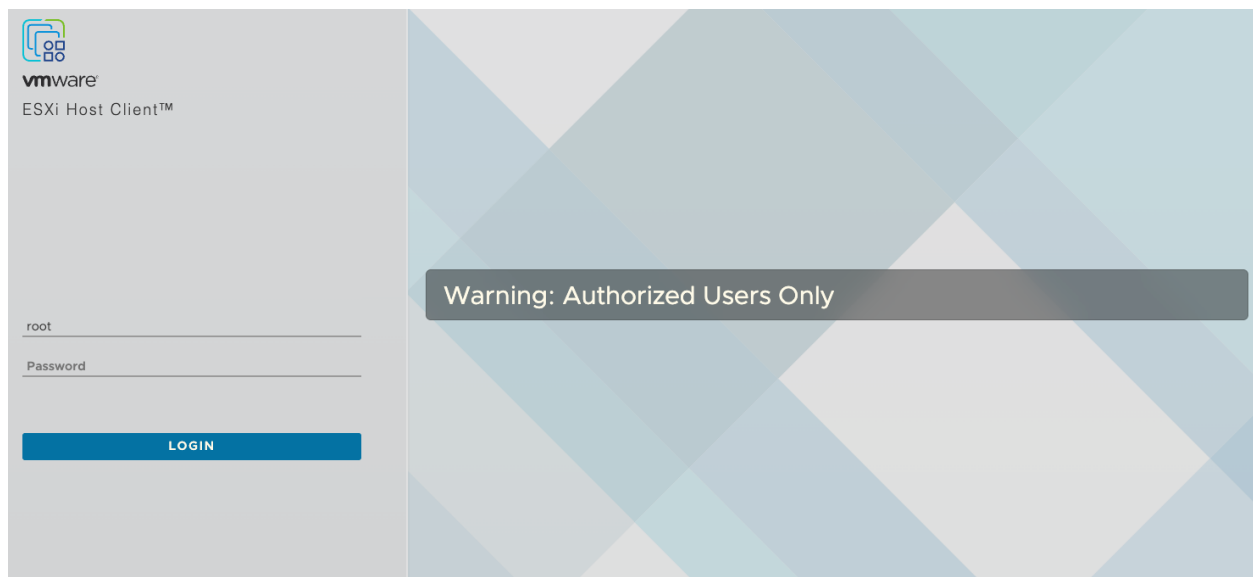
| Concept d'interface utilisateur         | Code de variable de balise méta  | Sortie  |
|---|--|---|
| Image personnalisée                     | <pre>{logo src="https://site/logo.png" width="100" height="100" align="center"}My Secured ESXi Server Tooltip{/logo}</pre> | <p>Affiche une image <code>logo.png</code> de 100 × 100 pixels centrée horizontalement au-dessus du bloc de messages. Un titre d'info-bulle accessible de <code>My Secured ESXi Server Tooltip</code> est ajouté à l'image.</p> <hr/> <p><b>Note</b> Assurez-vous d'utiliser les attributs <code>width</code>, <code>height</code> et <code>align</code>, bien qu'ils soient facultatifs. Tous les formats d'image Web sont pris en charge.</p> |
| Case à cocher Contrat de l'utilisateur  | <pre>{accept}Please accept the terms{/ accept}</pre>   | Affiche une case à cocher avec l'étiquette « Veuillez accepter les conditions » au bas du contenu du message.   |
| Message d'erreur d'acceptation appliqué | <pre>{mustaccept}You must agree before logging into the system{/ mustaccept}</pre>   | Ajoute la validation du formulaire pour exiger que l'utilisateur coche la case avant de se connecter. Si l'utilisateur ne coche pas la case, le message « Vous devez accepter avant de vous connecter au système » s'affiche au-dessus du bouton de connexion.  |

## Exemples

### Markdown simple

Un élément Markdown d'une seule ligne pour un message uniquement en texte simple

```
## Warning: Authorized Users Only
```



### Markdown avancé

Exemple de Markdown avancé pour une société de stockage cloud fictive « Vaulted », avec un logo, des liens et une case à cocher d'acceptation requise sur le formulaire.

```
## Warning: Authorized Users Only

The information on this host is the property of "Vaulted Storage" (sample organization)
and is protected under sovereign intellectual property rights.

You must be assigned an account on this computer to access information and are only allowed
to access information defined by the system administrators.

All activities are monitored and trespassing violators will be reported to a federal
law enforcement agency.

### Policy bulletins
Please refer to the helpful links below on end user protection guidelines.

* [Privacy addendum] (https://en.wikipedia.org/wiki/Computer_security)
* [Terms of Use] (https://en.wikipedia.org/wiki/Terms_of_service#:~:text=Terms%20of%20service%20(also%20known,to%20use%20the%20offered%20service.)

...

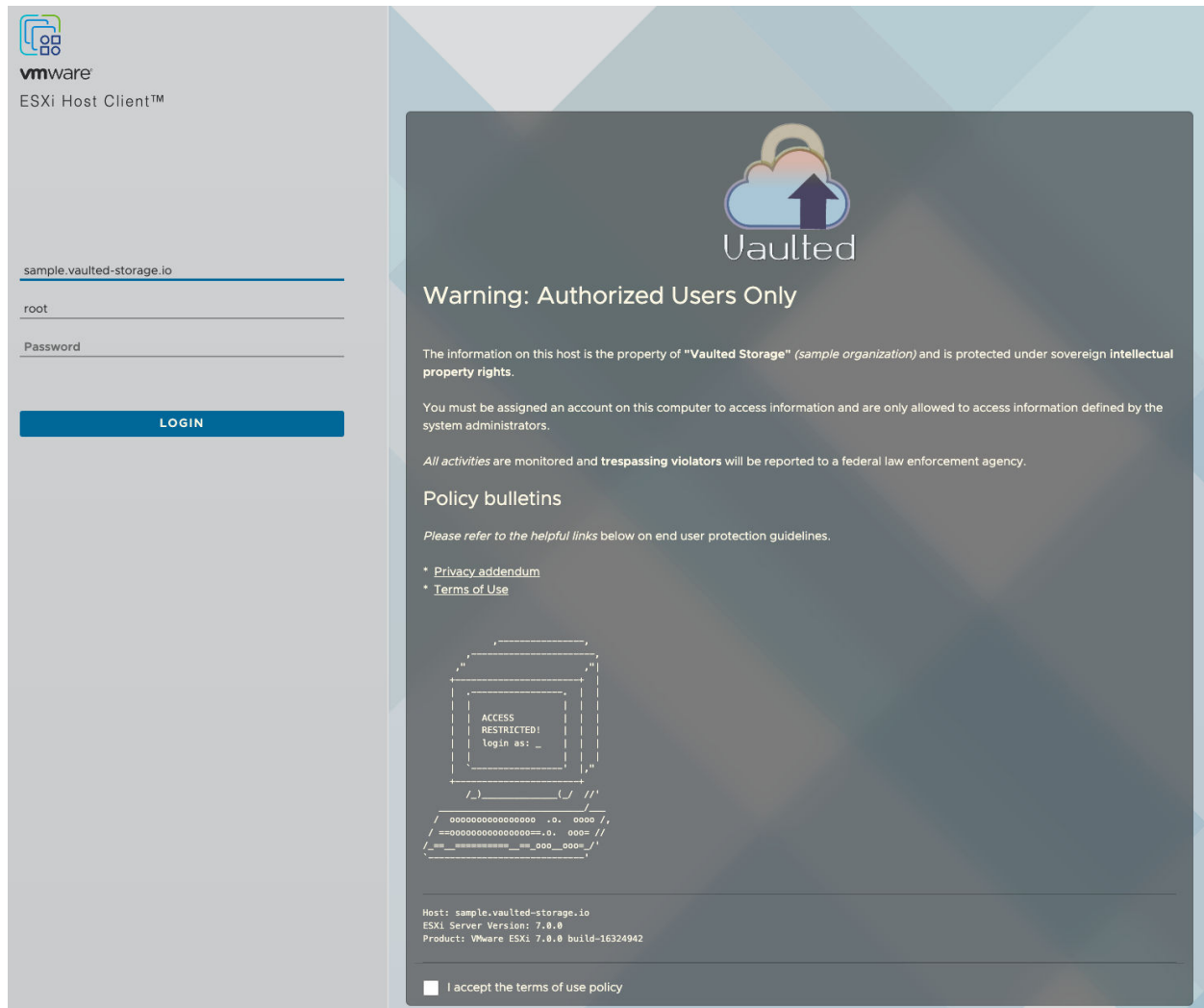
      ,-----,
    ,-----,
  ,-----,
+-----+
| .----- . |
| | ACCESS | |
| | RESTRICTED! | |
| | login as: _ | |
| | | | |
| |-----' |,"
+-----+
/_ ) _____ ( _ / // '
/
/ ooooooooooooooooo .o. oooo /,
/ ==ooooooooooooooooo==.o. ooo= //
/_ == _____ ==_ooo_ooo=_/'
'-----'

-----
Host: {hostname}
ESXi Server Version: {esxversion}
Product: {esxproduct}
-----
...

{logo align="center" width="200" height="200" src="https://i.postimg.cc/y6wZXTpm/vaulted-logo-white-text.png"}Vaulted Enterprise Storage{/logo}

{accept}I accept the terms of use policy{/accept}

{mustaccept}User must check terms of use to login. LOG OFF immediately if you do not agree to
the conditions stated in the warning.{/mustaccept}
```



## Quitter ou rejoindre le programme d'amélioration du produit dans VMware Host Client

Vous pouvez participer au programme d'amélioration du produit (CEIP) pour fournir des commentaires ou des informations anonymes à VMware afin d'améliorer la qualité, la fiabilité et les fonctionnalités des produits et services VMware.

Vous pouvez, à tout moment, décider de quitter le CEIP (Programme d'amélioration du produit) ou le rejoindre.

Les détails concernant les données recueillies via le CEIP et les fins auxquelles elles sont utilisées par VMware sont définis dans le Centre d'approbation et d'assurance à l'adresse <http://www.vmware.com/trustvmware/ceip.html>.

### Procédure

- 1 Pour quitter ou rejoindre le CEIP, cliquez sur le nom d'utilisateur en haut de la page VMware Host Client.

- 2 Sélectionnez **Paramètres > Envoyer les statistiques d'utilisation**, pour quitter ou rejoindre le CEIP.

# Gestion des hôtes avec VMware Host Client

# 3

Avec VMware Host Client, vous pouvez gérer individuellement des hôtes ESXi pendant les mises à niveau de vCenter Server ou quand vCenter Server cesse de répondre ou est indisponible.

VMware Host Client possède un ensemble essentiel de fonctions de dépannage qui vous permet d'effectuer des tâches sur l'hôte ESXi auquel vous êtes connecté si vCenter Server est indisponible. Ces fonctions comprennent, entre autres, la configuration des paramètres avancés de l'hôte, l'attribution des licences, la gestion des certificats, l'utilisation de ESXi Shell, l'activation du mode de verrouillage, etc.

Ce chapitre contient les rubriques suivantes :

- [Gérer les paramètres système dans VMware Host Client](#)
- [Gérer le matériel d'un hôte ESXi avec VMware Host Client](#)
- [Attribution de licences pour les hôtes ESXi](#)
- [Gérer les services dans VMware Host Client](#)
- [Gestion de la sécurité et des utilisateurs pour un hôte ESXi avec VMware Host Client](#)
- [Gérer des hôtes dans vCenter Server](#)
- [Redémarrer ou arrêter ESXi Host dans VMware Host Client](#)
- [Utilisation du ESXi Shell](#)
- [Mettre un hôte en mode de maintenance dans VMware Host Client](#)
- [Gérer les autorisations dans VMware Host Client](#)
- [Générer un bundle de support dans VMware Host Client](#)
- [Mode de verrouillage dans VMware Host Client](#)
- [Gérer des ressources CPU à l'aide de VMware Host Client](#)
- [Surveiller un hôte ESXi dans VMware Host Client](#)

## Gérer les paramètres système dans VMware Host Client

Avec VMware Host Client, vous pouvez gérer les paramètres d'hôte avancés, attribuer ou supprimer des licences pour votre hôte, configurer les stratégies de début et de fin des services de l'hôte, et gérer la configuration de l'heure et de la date pour l'hôte.

## Gérer les paramètres avancés dans VMware Host Client

Vous pouvez modifier les paramètres d'un hôte avec VMware Host Client.

---

**Attention** La modification des options avancées est considérée comme non prise en charge sauf si l'assistance technique VMware ou un article KB vous demandent de le faire. Dans tous les autres cas, la modification de ces options est considérée comme non prise en charge. Dans la plupart des cas, les paramètres par défaut donnent un résultat optimal.

---

### Procédure

- 1 Cliquez sur **Gérer** dans l'inventaire VMware Host Client et cliquez sur **Système**.
- 2 Cliquez sur **Paramètres avancés**.
- 3 Cliquez avec le bouton droit sur l'élément approprié de la liste et sélectionnez **Modifier l'option** dans le menu déroulant.  
La boîte de dialogue **Modifier l'option** apparaît.
- 4 Modifiez la valeur et cliquez sur **Enregistrer** pour appliquer les modifications.
- 5 (Facultatif) Cliquez avec le bouton droit sur l'élément approprié de la liste et sélectionnez **Réinitialiser les valeurs par défaut** pour revenir aux paramètres d'origine de l'élément.

## Créer un message de bienvenue initial pour l'interface utilisateur de la console directe (DCUI) et VMware Host Client

À l'aide de VMware Host Client, vous pouvez créer un message de bienvenue qui s'affiche sur l'écran initial de l'interface utilisateur de la console directe (DCUI) et dans la fenêtre de connexion de VMware Host Client. Vous pouvez également créer un message de bienvenue qui s'affiche lorsqu'un utilisateur se connecte à VMware Host Client et décider s'il convient d'afficher le message de bienvenue.

## Procédure

- 1 Cliquez sur **Gérer** dans l'inventaire VMware Host Client et cliquez sur **Paramètres avancés**.

| Option   | Action   |
|--|--|
| Créez un message de bienvenue qui s'affiche avant de vous connecter à DCUI et à VMware Host Client   | <ol style="list-style-type: none"> <li>a Entrez <b>Annotations.WelcomeMessage</b> dans la zone de texte <b>Rechercher</b>, puis cliquez sur l'icône <b>Rechercher</b>.</li> <li>b Cliquez avec le bouton droit de la souris sur <b>Annotations.WelcomeMessage</b> et sélectionnez <b>Modifier l'option</b> dans le menu déroulant.<br/><br/>La boîte de dialogue <b>Modifier l'option</b> s'ouvre.</li> <li>c Dans la zone de texte <b>Nouvelle valeur</b>, entrez le message de bienvenue.<br/><br/>Pour définir le message par défaut, laissez la zone de texte <b>Nouvelle valeur</b> vide.</li> </ol>  |
| Créez un message de bienvenue qui s'affiche après votre connexion à VMware Host Client               | <ol style="list-style-type: none"> <li>a Entrez <b>UserVars.HostClientWelcomeMessage</b> dans la zone de texte <b>Rechercher</b>, puis cliquez sur l'icône <b>Rechercher</b>.</li> <li>b Cliquez avec le bouton droit de la souris sur <b>UserVars.HostClientWelcomeMessage</b> et sélectionnez <b>Modifier l'option</b> dans le menu déroulant.<br/><br/>La boîte de dialogue <b>Modifier l'option</b> s'ouvre.</li> <li>c Dans la zone de texte <b>Nouvelle valeur</b>, entrez le message de bienvenue.<br/><br/>Pour définir le message par défaut, laissez la zone de texte <b>Nouvelle valeur</b> vide.</li> </ol>  |
| Activez ou désactivez l'affichage du message de bienvenue après votre connexion à VMware Host Client | <ol style="list-style-type: none"> <li>a Entrez <b>UserVars.HostClientEnableMessage</b> dans la zone de texte <b>Rechercher</b>, puis cliquez sur l'icône <b>Rechercher</b>.</li> <li>b Cliquez avec le bouton droit de la souris sur <b>UserVars.HostClientEnableMOTDNotification</b> et sélectionnez <b>Modifier l'option</b> dans le menu déroulant.<br/><br/>La boîte de dialogue <b>Modifier l'option</b> s'ouvre.</li> <li>c Dans la zone de texte <b>Nouvelle valeur</b>, entrez la nouvelle valeur.<br/><br/>Une valeur de zéro (0) désactive l'apparence du message de bienvenue.<br/><br/>Une valeur égale à un (1) active l'affichage du message de bienvenue.</li> </ol> |

- 2 Cliquez sur **Enregistrer**.
- 3 (Facultatif) Pour réinitialiser le paramètre de clé à la valeur par défaut, cliquez avec le bouton droit sur la clé appropriée dans la liste, puis sélectionnez l'option **Réinitialiser sur les paramètres par défaut**.

## Configurer le délai d'expiration de session de l'interface utilisateur VMware Host Client

Dans VMware Host Client, la session de l'interface utilisateur expire automatiquement toutes les 15 minutes, puis vous devez vous reconnecter à VMware Host Client.

Vous pouvez augmenter le délai d'inactivité par défaut en modifiant un paramètre de configuration avancé. La valeur par défaut est 900 secondes.

## Procédure

- ◆ Configurez le délai d'expiration de session de l'interface utilisateur.

| Option   | Action  |
|--|---|
| Dans Paramètres avancés de VMware Host Client      | <p>a Cliquez sur <b>Gérer</b> dans l'inventaire VMware Host Client, puis sur <b>Paramètres avancés</b></p> <p>b Entrez <code>UserVars.HostClientSessionTimeout</code> dans la zone de texte <b>Rechercher</b>, puis cliquez sur l'icône <b>Rechercher</b>.</p> <p>c Cliquez avec le bouton droit de la souris sur <code>UserVars.HostClientSessionTimeout</code> et sélectionnez <b>Modifier l'option</b> dans le menu déroulant.</p> <p>La boîte de dialogue <b>Modifier l'option</b> s'ouvre.</p> <p>d Dans la zone de texte <b>Nouvelle valeur</b>, entrez le paramètre de délai d'expiration en secondes.</p> <hr/> <p><b>Note</b> Une valeur de zéro (0) désactive le délai d'expiration.</p> <p>e Cliquez sur <b>Enregistrer</b>.</p> <p>f (Facultatif) Pour réinitialiser le paramètre de clé à la valeur par défaut, cliquez avec le bouton droit sur la clé appropriée dans la liste, puis sélectionnez l'option <b>Réinitialiser sur les paramètres par défaut</b>.</p> |
| Dans le menu déroulant Paramètres de l'utilisateur | <p>a Dans le haut de la fenêtre de VMware Host Client, cliquez sur le nom d'utilisateur et sélectionnez <b>Paramètres &gt; Délai d'expiration de l'application &gt;</b>.</p> <p>b Pour spécifier le délai d'inactivité, sélectionnez la durée.</p> <p>c Pour désactiver le délai d'inactivité, sélectionnez <code>Off</code>.</p>   |

## Configurer le délai d'expiration de session SOAP dans VMware Host Client

Dans VMware Host Client, vous pouvez configurer le délai d'expiration de la session SOAP.

### Procédure

- 1 Cliquez sur **Gérer** dans l'inventaire VMware Host Client et cliquez sur **Paramètres avancés**.
- 2 Entrez `Config.HostAgent.vmacore.soap.sessionTimeout` dans la zone de texte **Rechercher**, puis cliquez sur l'icône **Rechercher**.
- 3 Cliquez avec le bouton droit de la souris sur `Config.HostAgent.vmacore.soap.sessionTimeout` et sélectionnez **Modifier l'option** dans le menu déroulant.  
La boîte de dialogue **Modifier l'option** s'ouvre.
- 4 Dans la zone de texte **Nouvelle valeur**, entrez le paramètre de délai d'expiration en secondes.  
Une valeur de zéro (0) désactive le délai d'expiration.
- 5 Cliquez sur **Enregistrer**.



- 6 (Facultatif) Pour réinitialiser le paramètre de clé à la valeur par défaut, cliquez avec le bouton droit sur la clé appropriée dans la liste, puis sélectionnez l'option **Réinitialiser sur les paramètres par défaut**.

## Configurer la politique de mot de passe et de verrouillage de compte dans VMware Host Client

Pour les hôtes ESXi, vous devez utiliser un mot de passe avec des exigences prédéfinies. Vous pouvez modifier la longueur de mot de passe requise et l'exigence de classes de caractères ou autoriser les phrases secrètes à l'aide de l'option avancée `Security.PasswordQualityControl`. Vous pouvez également définir le nombre de mots de passe à mémoriser pour chaque utilisateur à l'aide de l'option avancée `Security.PasswordHistory`. L'option avancée `Security.PasswordMaxDays` vous permet de définir le nombre maximal de jours entre les changements de mot de passe.

---

**Note** Effectuez toujours des tests supplémentaires après avoir modifié les paramètres du mot de passe par défaut.

---

Si vous tentez de vous connecter avec des informations d'identification incorrectes, la stratégie de verrouillage de compte spécifie quand et pendant combien de temps le système verrouille votre compte.

### Mots de passe d'ESXi

ESXi applique les exigences de mot de passe pour l'accès.

- Par défaut, lorsque vous créez un mot de passe, vous devez utiliser 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.
- Par défaut, le mot de passe doit contenir au moins 7 caractères et un maximum de 40 caractères.
- Les mots de passe ne doivent pas contenir un mot de dictionnaire ou une partie d'un mot de dictionnaire.
- Les mots de passe ne doivent pas contenir le nom d'utilisateur ou des parties du nom d'utilisateur.

---

**Note** 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 utilisés.

---

### Exemple de mots de passe ESXi

Les candidats de mot de passe suivants illustrent les mots de passe potentiels si l'option est définie comme suit :

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

Avec ce paramètre, un utilisateur est invité jusqu'à trois fois (retry=3) à entrer un nouveau mot de passe si celui-ci n'est pas suffisamment sécurisé ou si le mot de passe n'a pas été entré correctement deux fois. Les mots de passe avec une ou deux classes de caractères et les phrases de mot de passe ne sont pas autorisés, car les trois premiers éléments sont désactivés. Les mots de passe composés de trois et quatre classes de caractères exigent 7 caractères.

Les candidats de mot de passe suivants répondent aux exigences de mot de passe :

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

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

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

### Contrôle de qualité des mots de passe

Vous pouvez contrôler la qualité des mots de passe à l'aide de l'option avancée

`Security.PasswordQualityControl`.

`Security.PasswordQualityControl` consiste en plusieurs paramètres suivant ce modèle :

```
retry=N min=N0,N1,N2,N3,N4 max=N passphrase=N similar=permit|deny
```

| Paramètres de contrôle de la qualité des mots de passe | Description   | Par défaut                                      |
|--|---|---|
| <code>retry=N</code>                                   | Nombre de fois qu'un utilisateur doit fournir un nouveau mot de passe si le mot de passe est incorrect ou pas suffisamment fort.  | <code>retry=3</code>                            |
| <code>min=N0,N1,N2,N3,N4</code>                        | <p>Exigence de classes de caractères et de longueur minimale de phrase secrète.</p> <ul style="list-style-type: none"> <li>■ <code>N0</code> est la longueur minimale des mots de passe d'une classe de caractère spécifique.</li> <li>■ <code>N1</code> est la longueur minimale des mots de passe de deux classes de caractères.</li> <li>■ <code>N2</code> est la longueur minimale d'une phrase secrète.</li> <li>■ <code>N3</code> est la longueur minimale de trois classes de caractères.</li> <li>■ <code>N4</code> est la longueur minimale de quatre classes de caractères.</li> </ul> <p>Vous pouvez utiliser <code>disabled</code> pour interdire un mot de passe avec le nombre spécifié de classes de caractères.</p> | <code>min=disabled,disabled,disabled,7,7</code> |
| <code>max=N</code>                                     | Longueur maximale autorisée du mot de passe.  | <code>max=40</code>                             |
| <code>passphrase=N</code>                              | Nombre de mots requis pour une phrase secrète. Pour s'assurer que <code>passphrase</code> est reconnu, ne définissez pas <code>N2</code> du paramètre <code>min</code> sur <code>disabled</code> .  | <code>passphrase=3</code>                       |
| <code>similar=permit deny</code>                       | Indique si un mot de passe est autorisé à être similaire à l'ancien mot de passe. Pour utiliser ce paramètre, assurez-vous que vous avez défini l'option <code>Security.PasswordHistory</code> sur une valeur non nulle.  | <code>similar=deny</code>                       |

## Phrase secrète ESXi

Au lieu d'un mot de passe, vous pouvez utiliser une phrase secrète. Les phrases secrètes sont désactivées par défaut. Vous pouvez modifier le paramètre par défaut à l'aide de l'option avancée `Security.PasswordQualityControl`.

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

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

Cet exemple autorise les phrases secrètes d'au moins 16 caractères. La phrase secrète doit comporter au moins 3 mots, séparés par des espaces.

### Exemple d'historique de mots de passe et de stratégie de rotation

Pour mémoriser un historique de 5 mots de passe, définissez l'option `Security.PasswordHistory` sur 5.

Pour appliquer une stratégie de rotation des mots de passe de 90 jours, définissez l'option `Security.PasswordMaxDays` sur 90.

### Stratégie de verrouillage des comptes d'ESXi

Les utilisateurs sont verrouillés après un nombre prédéfini de tentatives de connexion infructueuses successives. Par défaut, les utilisateurs sont verrouillés après 5 tentatives infructueuses successives en 3 minutes et un compte verrouillé est déverrouillé automatiquement après 15 minutes par défaut. Vous pouvez modifier le nombre maximal de tentatives infructueuses autorisées et la période pendant laquelle le compte d'utilisateur est verrouillé à l'aide des options avancées `Security.AccountLockFailures` et `Security.AccountUnlockTime`.

Pour configurer les mots de passe d'administrateur et le comportement de verrouillage du compte, procédez comme suit.

#### Procédure

- 1 Cliquez sur **Gérer** dans l'inventaire VMware Host Client et cliquez sur **Paramètres avancés**.

| Option   | Action  |
|--|---|
| Configurez la longueur requise du mot de passe, la classe de caractères requise ou autorisez les phrases secrètes. | <ol style="list-style-type: none"> <li>Entrez <code>Security.PasswordQualityControl</code> dans la zone de texte <b>Rechercher</b>, puis cliquez sur l'icône <b>Rechercher</b>.</li> <li>Cliquez avec le bouton droit de la souris sur <code>Security.PasswordQualityControl</code> et sélectionnez <b>Modifier l'option</b> dans le menu déroulant.</li> </ol>   |
| Configurer le nombre de mots de passe à mémoriser pour chaque utilisateur  | <ol style="list-style-type: none"> <li>Entrez <code>Security.PasswordHistory</code> dans la zone de texte <b>Rechercher</b>, puis cliquez sur l'icône <b>Rechercher</b>.</li> <li>Cliquez avec le bouton droit de la souris sur <code>Security.PasswordHistory</code> et sélectionnez <b>Modifier l'option</b> dans le menu déroulant.</li> </ol> <p><b>Note</b> Zéro désactive l'historique des mots de passe.</p> |
| Configurer le nombre maximal de jours entre les changements de mot de passe  | <ol style="list-style-type: none"> <li>Entrez <code>Security.PasswordMaxDays</code> dans la zone de texte <b>Rechercher</b>, puis cliquez sur l'icône <b>Rechercher</b>.</li> <li>Cliquez avec le bouton droit de la souris sur <code>Security.PasswordMaxDays</code> et sélectionnez <b>Modifier l'option</b> dans le menu déroulant.</li> </ol>   |

| Option  | Action  |
|---|---|
| Configurez le nombre de tentatives de connexion infructueuses autorisées avant le verrouillage. | <p>a Entrez <b>Security.AccountLockFailures</b> dans la zone de texte <b>Rechercher</b>, puis cliquez sur l'icône <b>Rechercher</b>.</p> <p>b Cliquez avec le bouton droit de la souris sur <b>Security.AccountLockFailures</b> et sélectionnez <b>Modifier l'option</b> dans le menu déroulant.</p> <hr/> <p><b>Note</b> Zéro (0) désactive le verrouillage du compte.</p> |
| Configurer la période pendant laquelle le compte de l'utilisateur est verrouillé                | <p>a Entrez <b>Security.AccountUnlockTime</b> dans la zone de texte <b>Rechercher</b>, puis cliquez sur l'icône <b>Rechercher</b>.</p> <p>b Cliquez avec le bouton droit de la souris sur <b>Security.AccountUnlockTime</b> et sélectionnez <b>Modifier l'option</b> dans le menu déroulant.</p>  |

La boîte de dialogue **Modifier l'option** s'ouvre.

- 1 Dans la zone de texte **Nouvelle valeur**, entrez le nouveau paramètre.
- 3 Cliquez sur **Enregistrer**.
- 4 (Facultatif) Pour réinitialiser le paramètre de clé à la valeur par défaut, cliquez avec le bouton droit sur la clé appropriée dans la liste, puis sélectionnez l'option **Réinitialiser sur les paramètres par défaut**.

## Configurer Syslog dans VMware Host Client

Pour configurer le service Syslog, vous pouvez utiliser VMware Host Client.

### Procédure

- 1 Cliquez sur **Gérer** dans l'inventaire VMware Host Client et cliquez sur **Paramètres avancés**.
- 2 Dans la zone de texte **Rechercher**, entrez le nom du paramètre que vous souhaitez modifier et cliquez sur l'icône **Rechercher**.

| Option                                | Description  |
|---------------------------------------|--|
| <b>Syslog.global.LogHost</b>          | <p>Hôte distant vers lequel les messages Syslog sont transférés et port sur lequel l'hôte distant reçoit les messages Syslog. Vous pouvez inclure le protocole et le port, par exemple, <code>protocol://hostName1:port</code> où <code>protocol</code> peut être <code>udp</code>, <code>tcp</code> ou <code>ssl</code>. Vous ne pouvez utiliser que le port 514 pour UDP. Le protocole <code>ssl</code> utilise TLS 1.2. Par exemple : <code>ssl://hostName1:1514</code>. La valeur de <code>port</code> peut être n'importe quel nombre décimal compris entre 1 et 65535.</p> <p>Bien qu'il n'existe aucune limite stricte au nombre d'hôtes distants pour recevoir des messages Syslog, il est recommandé de conserver le nombre d'hôtes distants à cinq ou moins.</p> |
| <b>Syslog.global.logCheckSSLCerts</b> | Appliquez la vérification des certificats SSL lorsque vous vous connectez à un hôte distant.   |
| <b>Syslog.global.defaultRotate</b>    | Nombre maximal d'archives à conserver. Vous pouvez définir ce nombre de façon globale et pour les sous-unités d'enregistrement automatique.  |

| Option                            | Description   |
|-----------------------------------|---|
| <b>Syslog.global.defaultSize</b>  | Taille par défaut du journal, en Ko, avant que le système n'effectue la rotation des journaux. Vous pouvez définir ce nombre de façon globale et pour les sous-unités d'enregistrement automatique.   |
| <b>Syslog.global.LogDir</b>       | Répertoire dans lequel sont stockés les journaux. Le répertoire peut se trouver sur des volumes NFS ou VMFS montés. Seul le répertoire <code>/scratch</code> situé sur le système de fichiers local subsiste après des redémarrages. Spécifiez le répertoire sous la forme <code>[nom_banque_de_données]chemin_du_fichier</code> , le chemin étant relatif à la racine du volume qui assure la sauvegarde de la banque de données. Par exemple, le chemin <code>[storage1] /systemlogs</code> crée un mappage vers le chemin <code>/vmfs/volumes/storage1/systemlogs</code> . |
| <b>Syslog.global.logDirUnique</b> | Lorsque vous sélectionnez cette option, un sous-répertoire est créé portant le nom de l'hôte ESXi dans le répertoire spécifié par <b>Syslog.global.LogDir</b> . Il est utile d'avoir un répertoire unique si le même répertoire NFS est utilisé par plusieurs hôtes ESXi.   |

- 3 Cliquez avec le bouton droit de la souris sur le nom du paramètre, puis sélectionnez **Modifier l'option** dans le menu déroulant.

La boîte de dialogue **Modifier l'option** s'ouvre.

- 4 Pour effectuer la vérification des certificats SSL lorsque vous vous connectez à un hôte distant, cliquez sur **True** dans **Nouvelle valeur**.
- 5 Cliquez sur **Enregistrer**.
- 6 (Facultatif) Pour réinitialiser le paramètre de clé à la valeur par défaut, cliquez avec le bouton droit sur la clé appropriée dans la liste, puis sélectionnez l'option **Réinitialiser sur les paramètres par défaut**.

## Configurer les options de clé TLS/SSL avancées

Vous pouvez configurer les protocoles de sécurité et les algorithmes de chiffrement utilisés pour chiffrer les communications avec l'hôte ESXi.

Pour plus d'informations, consultez l'article de la base de connaissances VMware à l'adresse <https://kb.vmware.com/s/article/79476>.

La clé TLS (Transport Layer Security) sécurise les communications avec l'hôte à l'aide du protocole TLS. Lors du premier démarrage, l'hôte ESXi génère la clé TLS en tant que clé RSA 2 048 bits. Actuellement, ESXi n'implémente pas la génération automatique de clés ECDSA pour TLS. La clé privée TLS n'est pas destinée à être prise en charge par l'administrateur.

La clé SSH sécurise les communications avec l'hôte ESXi à l'aide du protocole SSH. Lors du premier démarrage, le système génère la clé SSH sous la forme d'une clé RSA 2 048 bits. Le serveur SSH est désactivé par défaut. L'accès SSH est conçu principalement à des fins de dépannage. La clé SSH n'est pas destinée à être prise en charge par l'administrateur. La connexion via SSH nécessite des privilèges d'administration équivalents au contrôle complet de l'hôte. Pour activer l'accès SSH, reportez-vous à la section [Activer Secure Shell \(SSH\) dans VMware Host Client](#).

Vous pouvez configurer les paramètres de clé de sécurité de l'hôte ESXi suivants.

**Note** Le paramètre de clé de sécurité UserVars.ESXiVPsAllowedCiphers affecte uniquement les filtres d'E/S.

| Touche  | Par défaut  | Description   |
|---|---|---|
| UserVars.ESXiVPsAllowedCiphers                | !<br>aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES | Chaîne de contrôle de chiffrement par défaut.   |
| Config.HostAgent.ssl.keyStore.allowAny        | False   | Vous pouvez ajouter n'importe quel certificat au magasin d'approbations de l'autorité de certification ESXi.  |
| Config.HostAgent.ssl.keyStore.allowSelfSigned | False   | Vous pouvez ajouter des certificats auto-signés non émis par une autorité de certification au magasin d'approbations de l'autorité de certification ESXi, c'est-à-dire des certificats pour lesquels le bit d'autorité de certification n'est pas activé. |
| Config.HostAgent.ssl.keyStore.discardLeaf     | True  | Ignore les certificats feuille ajoutés au magasin d'approbations de l'autorité de certification ESXi.   |

Pour configurer les paramètres de clé de sécurité ESXi :

#### Procédure

- 1 Cliquez sur **Gérer** dans l'inventaire VMware Host Client et cliquez sur **Paramètres avancés**.
- 2 Entrez la clé de sécurité dans la zone de texte **Rechercher** et cliquez sur l'icône **Rechercher**.
- 3 Cliquez avec le bouton droit sur la clé de sécurité et sélectionnez **Modifier l'option** dans le menu déroulant.

La boîte de dialogue **Modifier l'option** s'ouvre.

- 4 Dans le champ **Nouvelle valeur**, entrez la nouvelle valeur et cliquez sur **Enregistrer**.

- 5 (Facultatif) Pour réinitialiser le paramètre de clé à la valeur par défaut, cliquez avec le bouton droit sur la clé appropriée dans la liste, puis sélectionnez l'option **Réinitialiser sur les paramètres par défaut**.

## Configurer la mise à zéro de la mémoire userworld

VMware Host Client vous permet d'utiliser l'option avancée `Mem.MemEagerZero` pour déterminer la manière dont les pages sont mises à zéro pour les machines virtuelles et les applications de l'espace utilisateur.

Pour mettre à zéro toutes les pages lorsqu'elles sont allouées à des machines virtuelles et à des applications d'espace utilisateur, définissez `Mem.MemEagerZero` sur un (1). Si la mémoire n'est pas réutilisée, ce paramètre empêche d'exposer les informations d'une machine virtuelle ou d'applications d'espace utilisateur à d'autres clients tout en conservant le contenu précédent en mémoire.

Lorsque vous définissez `Mem.MemEagerZero` sur 1, les pages sont mises à zéro lors de la fermeture d'une application de l'espace utilisateur. Pour les machines virtuelles, ces pages sont mises à zéro si :

- La machine virtuelle est mise hors tension.
- Les pages de machine virtuelle sont migrées.
- L'hôte ESXi récupère la mémoire des machines virtuelles.

---

**Note** Pour les machines virtuelles, vous pouvez obtenir ce comportement en définissant l'option avancée `sched.mem.eagerZero` sur **TRUE**.

Pour plus d'informations sur la configuration des options avancées de machine virtuelle, reportez-vous à la documentation *Gestion des ressources vSphere*.

---

Pour configurer la mise à zéro de la mémoire userworld, procédez comme suit.

### Procédure

- 1 Cliquez sur **Gérer** dans l'inventaire VMware Host Client et cliquez sur **Paramètres avancés**.
- 2 Entrez **Mem.MemEagerZero** dans la zone de texte **Rechercher**, puis cliquez sur l'icône **Rechercher**.
- 3 Cliquez avec le bouton droit de la souris sur `Mem.MemEagerZero` et sélectionnez **Modifier l'option** dans le menu déroulant.  
La boîte de dialogue **Modifier l'option** s'ouvre.
- 4 Dans la zone de texte **Nouvelle valeur**, entrez la nouvelle valeur.  
La valeur par défaut est zéro (0).
- 5 Cliquez sur **Enregistrer**.



- 6 (Facultatif) Pour réinitialiser le paramètre de clé à la valeur par défaut, cliquez avec le bouton droit sur la clé appropriée dans la liste, puis sélectionnez l'option **Réinitialiser sur les paramètres par défaut**.

## Modifier la configuration du démarrage automatique dans VMware Host Client

Configurez les options de démarrage automatique de l'hôte ESXi pour définir à quel moment l'hôte démarre et s'arrête.

### Procédure

- 1 Cliquez sur **Gérer** dans l'inventaire VMware Host Client et cliquez sur **Système**.
- 2 Cliquez sur **Démarrage automatique**.
- 3 Cliquez sur **Modifier les paramètres**.
- 4 Sélectionnez **Oui** pour permettre la modification de la configuration du démarrage automatique.

| Option                          | Description   |
|---------------------------------|---|
| Délai de démarrage              | Une fois l'hôte ESXi démarré, les machines virtuelles configurées pour démarrer automatiquement s'enclenchent. L'hôte ESXi démarre la première machine virtuelle, puis attend le délai spécifié pour démarrer la machine virtuelle suivante.  |
| Délai d'arrêt                   | Le délai d'arrêt est la durée maximale pendant laquelle l'hôte ESXi attend la fin d'une commande d'arrêt. Les machines virtuelles s'arrêtent dans l'ordre contraire à leur ordre de démarrage. Une fois que l'hôte ESXi arrête la première machine virtuelle dans le délai spécifié, l'hôte arrête la machine virtuelle suivante. Si une machine virtuelle ne s'arrête pas dans le délai spécifié, l'hôte exécute une commande de mise hors tension, puis commence à arrêter la machine virtuelle suivante. L'hôte ESXi s'arrête uniquement lorsque toutes les machines virtuelles sont arrêtées. |
| Arrêter l'action                | Sélectionnez une action d'arrêt applicable aux machines virtuelles sur l'hôte lorsque celui-ci s'éteint. <ul style="list-style-type: none"> <li>■ <b>Système par défaut</b></li> <li>■ <b>Mettre hors tension</b></li> <li>■ <b>Interrompre</b></li> <li>■ <b>Arrêter</b></li> </ul>  |
| Attendre le signal de pulsation | Sélectionnez <b>Oui</b> pour activer l'option <b>Attendre le signal de pulsation</b> . Vous pouvez utiliser cette option si VMware Tools est installé sur le système d'exploitation invité de la machine virtuelle. Une fois que l'hôte ESXi met sous tension la première machine virtuelle, l'hôte met immédiatement sous tension la machine virtuelle suivante. L'ordre de démarrage dans lequel les machines virtuelles sont mises sous tension continue après que la machine virtuelle reçoit le premier signal de pulsation.   |

Si vous définissez une option de délai sur -1, le système utilise l'option par défaut.

- 5 Cliquez sur **Enregistrer**.

## Modifier la configuration de l'heure d'un hôte ESXi dans VMware Host Client

À l'aide de VMware Host Client, vous pouvez configurer manuellement les paramètres d'heure d'un hôte ou synchroniser la date et l'heure de l'hôte avec un serveur NTP ou PTP. NTP fournit une précision de temporisation de l'ordre de la milliseconde et PTP conserve cette précision de temporisation.

Le service NTP sur l'hôte relève périodiquement le temps et la date à partir du serveur NTP. Vous pouvez utiliser les boutons **Démarrer**, **Arrêter** ou **Redémarrer** pour modifier l'état du service NTP sur l'hôte à tout moment, quelle que soit la stratégie de démarrage sélectionnée pour le service NTP.

PTP provisionne une synchronisation de l'heure précise pour les machines virtuelles d'un réseau. Pour modifier le service PTP sur l'hôte à tout moment, vous pouvez utiliser les boutons **Démarrer**, **Arrêter** ou **Redémarrer**. Le démarrage ou l'arrêt du service PTP active ou désactive automatiquement PTP. Pour appliquer la modification lorsque vous activez ou désactivez le protocole PTP manuellement, démarrez ou arrêtez le service PTP.

Pour plus d'informations sur les services, reportez-vous à la section [Gérer les services dans VMware Host Client](#).

---

**Note** Les services NTP et PTP ne peuvent pas s'exécuter simultanément.

---

### Procédure

- 1 Cliquez sur **Gérer** dans l'inventaire VMware Host Client.
- 2 Dans l'onglet **Système**, cliquez sur **Date et heure**.

### 3 Définissez la date et l'heure de l'hôte.

| Option  | Action   |
|---|--|
| Configurer manuellement la date et l'heure sur cet hôte                   | <ol style="list-style-type: none"> <li> Cliquez sur <b>Modifier les paramètres NTP</b>.<br/>La boîte de dialogue <b>Modifier les paramètres NTP</b> s'affiche.</li> <li> Réglez l'heure et la date de l'hôte manuellement.</li> <li> Cliquez sur <b>Enregistrer</b>.</li> </ol>  |
| Utilisez le protocole NTP (Network Time Protocol) (activer le client NTP) | <ol style="list-style-type: none"> <li> Cliquez sur <b>Modifier les paramètres NTP</b>.<br/>La boîte de dialogue <b>Modifier les paramètres NTP</b> s'affiche.</li> <li> Sélectionnez la case d'option <b>Utiliser le protocole NTP (Network Time Protocol)</b>.</li> <li> Dans la zone de texte <b>Serveurs NTP</b>,, entrez les adresses IP ou les noms d'hôte des serveurs NTP que vous souhaitez utiliser.</li> <li> Dans le menu déroulant <b>Stratégie de démarrage du service NTP</b>, sélectionnez une option pour démarrer et arrêter le service NTP sur l'hôte. <ul style="list-style-type: none"> <li> ■ <b>Démarrer et arrêter avec l'utilisation de port.</b> Démarre ou arrête le service NTP lorsque le port client NTP est activé ou désactivé pour l'accès au profil de sécurité de l'hôte.</li> <li> ■ <b>Démarrer et arrêter avec l'hôte</b> - Démarre et arrête le service NTP lorsque l'hôte se met sous tension ou s'arrête.</li> <li> ■ <b>Démarrer et arrêter manuellement.</b> Active le démarrage et l'arrêt manuels du service NTP. Si vous sélectionnez la stratégie <b>Démarrer et arrêter manuellement</b>, l'état du service NTP change uniquement quand vous utilisez les contrôles de l'interface utilisateur.</li> </ul> </li> <li> Cliquez sur <b>Enregistrer</b>.</li> </ol> |
| Utiliser le protocole PTP (Activer le client PTP)                         | <ol style="list-style-type: none"> <li> Cliquez sur <b>Modifier les paramètres PTP</b>.</li> <li> Cochez la case <b>Activer</b>.</li> <li> Dans le menu déroulant <b>Interface réseau</b>, sélectionnez une interface réseau.<br/><br/>IPv4 et le masque de sous-réseau s'affichent.</li> <li> Cliquez sur <b>Enregistrer</b>.</li> </ol>  |

## Gérer le matériel d'un hôte ESXi avec VMware Host Client

Lorsque vous vous connectez à un hôte ESXi avec VMware Host Client, vous pouvez gérer les périphériques PCI et configurer les paramètres de gestion de l'alimentation.

### Règles de gestion de l'alimentation de l'hôte

Vous pouvez utiliser de puissantes fonctionnalités de gestion dans ESXi fournies par le matériel hôte fournit pour trouver le meilleur équilibre entre performance et puissance. Vous pouvez contrôler la manière dont ESXi utilise ces fonctions en sélectionnant une stratégie de gestion de l'alimentation.

La sélection d'une stratégie « haute performance » offre plus de performances absolues mais à un rendement inférieur (performance par watt). Les stratégies de faible alimentation offrent moins de performances absolues, mais à un rendement supérieur.

Vous pouvez sélectionner une stratégie pour l'hôte que vous gérez en utilisant VMware Host Client. Si vous ne sélectionnez pas une règle, ESXi utilise Équilibré par défaut.

**Tableau 3-1. Règles de gestion de l'alimentation de CPU**

| Règle de gestion de l'alimentation | Description  |
|------------------------------------|--|
| Haute performance                  | Ne pas utiliser les fonctionnalités de gestion de l'alimentation.  |
| Équilibré (valeur par défaut)      | Réduire la consommation énergétique en faisant le moins de compromis sur la performance                              |
| Faible alimentation                | Réduire la consommation d'énergie et risquer une faible performance  |
| Personnalisé                       | Stratégie de gestion de l'alimentation définie par l'utilisateur. La configuration avancée est désormais disponible. |

Lorsqu'un CPU s'exécute à basse fréquence, il peut également s'exécuter à une tension plus faible, ce qui permet de réaliser des économies d'énergie. Ce type de gestion de l'alimentation est généralement appelé Dynamic Voltage and Frequency Scaling (DVFS - Cadrage dynamique de tension et de fréquence). ESXi tente d'ajuster les fréquences de processeur pour que les performances des machines virtuelles ne soient pas affectées.

Lorsqu'un CPU est inactif, ESXi peut appliquer des états de longue inactivité (appelés état C). Plus l'état C correspond à une longue activité, moins le CPU consomme d'énergie, mais le délai de réactivation du CPU est plus long. Lorsqu'un CPU est inactif, ESXi applique un algorithme pour prévoir la durée d'inactivité et choisit un état C approprié. Dans les stratégies de gestion de l'alimentation qui n'utilisent pas les états C de longue inactivité, ESXi utilise uniquement l'état de plus courte inactivité C1 pour les CPU inactifs.

## Modifier les stratégies de gestion de l'alimentation dans VMware Host Client

Modifiez les stratégies de gestion de l'alimentation de l'hôte que vous gérez pour contrôler la consommation d'énergie de votre hôte.

### Procédure

- 1 Cliquez sur **Gérer** dans l'inventaire VMware Host Client et cliquez sur **Matériel**.
- 2 Cliquez sur **Gestion de l'alimentation** et cliquez sur **Modifier la stratégie**.  
Les stratégies de gestion de l'alimentation disponibles sont affichées.
- 3 Sélectionnez la stratégie à appliquer, puis cliquez sur **OK**.

## Changer l'étiquette de matériel dans VMware Host Client

Dans VMware Host Client, vous pouvez modifier l'étiquette de matériel de tous les périphériques de relais PCI disponibles sur une machine virtuelle. Les étiquettes de matériel permettent de limiter le placement des machines virtuelles à des instances matérielles spécifiques. Vous pouvez ajouter tous les périphériques disponibles avec la même étiquette de matériel ou une étiquette de matériel vide à une machine virtuelle.

### Procédure

- 1 Cliquez sur **Gérer** dans l'inventaire VMware Host Client.
- 2 Sous l'onglet **Matériel**, cliquez sur **Périphériques PCI**.
- 3 Sélectionnez un périphérique disponible dans la liste et cliquez sur **Étiquette de matériel**.  
Le relais bascule doit être actif pour le périphérique sélectionné.  
La boîte de dialogue **Modifier l'étiquette de matériel** s'affiche.
- 4 Modifiez l'étiquette de matériel et cliquez sur **Enregistrer** pour appliquer les modifications.

### Résultats

La nouvelle étiquette de matériel s'affiche dans la colonne Étiquette de matériel.

## Attribution de licences pour les hôtes ESXi

Les hôtes ESXi sont concédés sous licence vSphere. Chaque licence vSphere a une certaine capacité que vous pouvez utiliser pour attribuer des licences à plusieurs CPU physiques sur des hôtes ESXi.

À partir de vSphere 7.0, [une licence de CPU couvre un CPU jusqu'à 32 cœurs](#). Si le CPU comporte plus de 32 cœurs, vous avez besoin de licences de CPU supplémentaires.

| Nombre de CPU | Cœurs par CPU | Nombre de licences de CPU |
|---------------|---------------|---------------------------|
| 1             | 1-32          | 1                         |
| 2             | 1-32          | 2                         |
| 1             | 33-64         | 2                         |
| 2             | 33-64         | 4                         |

Lorsque vous attribuez une licence vSphere à un hôte, la quantité de capacité consommée est déterminée par le nombre de CPU physiques sur l'hôte et le nombre de cœurs dans chaque CPU physique. vSphere Desktop destiné aux environnements VDI est concédé sous licence par machine virtuelle.

Pour attribuer une licence à un hôte ESXi, vous devez lui attribuer une licence vSphere qui répond aux conditions préalables suivantes :

- La licence doit disposer d'une capacité suffisante pour la mise sous licence de tous les CPU physiques sur l'hôte.

- La licence doit prendre en charge toutes les fonctionnalités utilisées par l'hôte. Par exemple, si l'hôte est associé à un vSphere Distributed Switch, la licence que vous lui attribuez doit prendre en charge la fonctionnalité vSphere Distributed Switch.

Si vous essayez d'attribuer une licence qui a une capacité insuffisante ou qui ne prend pas en charge les fonctionnalités utilisées par l'hôte, l'attribution de la licence échoue.

Si vous utilisez le modèle de licence comportant jusqu'à 32 cœurs, vous pouvez attribuer une licence vSphere pour 10 CPU avec 32 cœurs à l'une des combinaisons d'hôtes suivantes :

- Cinq hôtes à 2 CPU avec 32 cœurs par CPU
- Cinq hôtes à 1 CPU avec 64 cœurs par CPU
- Deux hôtes à 2 CPU avec 48 cœurs par CPU et deux hôtes à 1 CPU avec 20 cœurs par CPU

Les CPU bicœur et quadricœur, tels que les CPU Intel qui combinent deux ou quatre CPU indépendants sur une puce unique, comptent pour un seul CPU.

## Mode d'évaluation

Une fois que vous avez installé ESXi, il fonctionne en mode d'évaluation pendant un maximum de 60 jours consécutifs. Une licence en mode d'évaluation fournit toutes les fonctionnalités de l'édition la plus récente du produit vSphere.

Lorsque vous attribuez une licence à un hôte ESXi, à tout moment avant l'expiration de la période d'évaluation, vous pouvez remettre l'hôte en mode d'évaluation afin d'explorer l'ensemble des fonctionnalités disponibles pendant la période d'évaluation restante.

Par exemple, si vous utilisez un hôte ESXi en mode d'évaluation pendant 20 jours, puis lui attribuez une licence vSphere Standard et le remettez en mode d'évaluation 5 jours plus tard, vous pouvez explorer l'intégralité des fonctionnalités disponibles pour l'hôte pendant les 35 jours restants de la période d'évaluation.

## Expiration de la licence et de la période d'évaluation

Pour les hôtes ESXi, l'expiration de la licence ou de la période d'évaluation entraîne la déconnexion de vCenter Server. Toutes les machines virtuelles sous tension continuent à fonctionner, mais vous ne pouvez pas mettre sous tension les machines virtuelles après leur mise hors tension. Vous ne pouvez pas modifier la configuration actuelle des fonctionnalités qui sont déjà utilisées. Vous ne pouvez pas utiliser les fonctionnalités qui n'ont pas été utilisées avant l'expiration de la licence.

---

**Note** En cas d'expiration des licences, une notification s'affiche 90 jours avant l'expiration de la licence.

---

## Attribution de licences aux hôtes ESXi après la mise à niveau

Si vous mettez à niveau un hôte ESXi vers une version qui commence par le même numéro, il n'est pas nécessaire de remplacer la licence existante par une nouvelle. Par exemple, si vous mettez à niveau un hôte ESXi 5.1 vers 5.5, vous pouvez utiliser la même licence pour l'hôte.

Si vous mettez à niveau un hôte ESXi vers une version majeure commençant par un numéro différent, la période d'évaluation redémarre et vous devez attribuer une nouvelle licence. Par exemple, si vous mettez à niveau un hôte ESXi 5.x vers 6.x, vous devez attribuer une licence vSphere 6.x à l'hôte.

## vSphere Desktop

vSphere Desktop est destiné aux environnements VDI tels qu'Horizon View. L'utilisation des licences vSphere Desktop équivaut au nombre total de machines virtuelles de poste de travail sous tension exécutées sur les hôtes auxquels une licence vSphere Desktop est attribuée.

## Afficher les informations relatives aux licences de l'environnement VMware Host Client

Vous pouvez afficher les licences disponibles dans VMware Host Client ainsi que les informations concernant les dates d'expiration, la clé de licence et les différentes fonctionnalités. Vous pouvez également afficher les produits et ressources disponibles.

### Procédure

- ◆ Cliquez sur **Gérer** dans l'inventaire VMware Host Client et cliquez sur **Licences**.

Vous pouvez afficher la clé de licence, la date d'expiration, ainsi que l'ensemble des fonctionnalités et ressources.

## Attribuer une clé de licence à un hôte ESXi dans VMware Host Client

À l'aide de VMware Host Client, vous pouvez attribuer une nouvelle clé de licence ou une clé existante à un hôte ESXi.

### Conditions préalables

Vérifiez que vous disposez du privilège **Global.Licenses**.

---

**Note** Si vous utilisez vCenter Server pour gérer votre hôte ESXi, la modification de vos licences peut uniquement s'effectuer à partir de vSphere Client.

---

### Procédure

- 1 Cliquez sur **Gérer** dans l'inventaire VMware Host Client et cliquez sur **Attribution de licence**.
- 2 Cliquez sur **Attribuer une licence**, entrez la clé de licence au format **xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx** et cliquez sur **Vérifier la licence**.
- 3 Cliquez sur **Attribuer la licence** pour enregistrer vos modifications.

## Supprimer une licence d'un hôte ESXi dans VMware Host Client

Pour garantir la conformité des modèles d'attribution de licence des produits que vous utilisez avec vSphere, vous devez supprimer toutes les licences non attribuées de l'inventaire. Si vous

avez divisé, combiné ou mis à niveau des licences dans Customer Connect, vous devez supprimer les anciennes licences.

Par exemple, supposons que vous ayez mis à niveau une licence vSphere de la version 6.5 vers la version 6.7 dans Customer Connect. Vous attribuez la licence aux hôtes ESXi 6.7. Après avoir attribué les nouvelles licences vSphere 6.7, vous devez supprimer l'ancienne licence vSphere 6.5 de l'inventaire.

#### Procédure

- 1 Cliquez sur **Gérer** dans l'inventaire VMware Host Client et cliquez sur **Attribution de licence**.
- 2 Cliquez sur **Supprimer la licence**, puis sur **OK**.

## Gérer les services dans VMware Host Client

Dans VMware Host Client, vous pouvez démarrer, arrêter et redémarrer les services qui sont exécutés sur l'hôte auquel vous êtes connecté et vous pouvez configurer la stratégie des services hôtes. Vous pouvez redémarrer des services lors d'une modification de la configuration des hôtes ou si vous suspectez la présence de problèmes fonctionnels ou de performances.

#### Procédure

- 1 Cliquez sur **Gérer** dans l'inventaire VMware Host Client et cliquez sur **Services**.
- 2 Dans la liste **Services**, sélectionnez un service.
- 3 Dans le menu déroulant **Actions**, sélectionnez une opération.
  - **Redémarrer**
  - **Démarrer**
  - **Arrêter**
- 4 (Facultatif) Dans le menu déroulant **Actions**, sélectionnez **Stratégie** et sélectionnez une option pour le service dans le menu.
  - **Démarrer et arrêter avec les ports du pare-feu**
  - **Démarrer et arrêter avec l'hôte**
  - **Démarrer et arrêter manuellement**

## Gestion de la sécurité et des utilisateurs pour un hôte ESXi avec VMware Host Client

L'architecture d'hyperviseur ESXi possède de nombreuses fonctionnalités intégrées que vous pouvez configurer pour améliorer la sécurité. Avec VMware Host Client, vous pouvez configurer des fonctionnalités telles qu'Active Directory, et vous pouvez également gérer les certificats.



## Gérer l'authentification des hôtes avec VMware Host Client

Lorsque vous vous connectez à un hôte ESXi avec VMware Host Client, vous pouvez vérifier si Active Directory et l'authentification par carte à puce sont activés et vous pouvez également associer l'hôte à un domaine du service d'annuaire.

### Associer un hôte ESXi à un domaine du service d'annuaire avec VMware Host Client

Pour utiliser un service d'annuaire pour votre hôte, vous devez associer 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 conteneur par défaut.
- **name.tld/container/path** (par exemple, **domain.com/OU1/OU2**) : le compte est créé sous une unité d'organisation (OU) précise.

Pour utiliser le service vSphere Authentication Proxy, consultez *Sécurité vSphere*.

#### Procédure

- 1 Cliquez sur **Gérer** dans l'inventaire VMware Host Client et cliquez sur **Sécurité et utilisateurs**.
- 2 Cliquez sur **Authentification** et cliquez sur **Associer le domaine**.
- 3 Entrez un nom de domaine.  
Utilisez le format **name.tld** ou **name.tld/container/path**.
- 4 Entrez le nom d'utilisateur et le mot de passe d'un utilisateur service d'annuaire autorisé à associer l'hôte au domaine, puis cliquez sur **Associer le domaine**.
- 5 (Facultatif) Si vous avez l'intention d'utiliser un proxy d'authentification, entrez l'adresse IP du serveur proxy et cliquez sur **Associer le domaine**.

### Utilisation d'Active Directory pour gérer des utilisateurs ESXi

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

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

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

## Utiliser vSphere Authentication Proxy

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

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

Pour plus d'informations sur les ports TCP utilisés par vSphere Authentication Proxy, reportez-vous à la section [#unique\\_39](#).

Reportez-vous à la documentation *Sécurité vSphere* pour plus d'informations sur l'activation de vSphere Authentication Proxy et sur les ports vCenter Server dont vSphere Authentication Proxy a besoin.

### Auto Deploy

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

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

Reportez-vous à la section [#unique\\_40](#).

### Autres hôtes ESXi

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

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

---

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

---

## Gérer les certificats des hôtes avec VMware Host Client

Lorsque vous vous connectez à un hôte ESXi avec VMware Host Client, vous pouvez afficher les détails des certificats de votre hôte, comme l'émetteur et la période de validité, et vous pouvez également importer de nouveaux certificats.

### Afficher les informations sur les certificats d'un hôte ESXi dans VMware Host Client

Vous pouvez utiliser les informations de certificat pour le débogage.

#### Procédure

- 1 Cliquez sur **Gérer** dans l'inventaire VMware Host Client et cliquez sur **Sécurité et utilisateurs**.
- 2 Cliquez sur **Certificats**.

Vous pouvez afficher les informations suivantes sur le certificat.

| Champ            | Description  |
|------------------|--|
| Émetteur         | Émetteur du certificat.                            |
| Non valide après | Date à laquelle le certificat expire.              |
| Non valide avant | Date à laquelle le certificat est généré.          |
| Objet            | Objet utilisé lors de la génération du certificat. |

### Importer un nouveau certificat pour un hôte ESXi dans VMware Host Client

Vous pouvez importer un certificat d'une autorité de certification de confiance quand vous êtes connecté à un hôte ESXi avec VMware Host Client.

#### Procédure

- 1 Cliquez sur **Gérer** dans l'inventaire VMware Host Client et cliquez sur **Sécurité et utilisateurs**.
- 2 Cliquez sur **Certificats** et cliquez sur **Importer un nouveau certificat**.

### 3 Générez une demande de signature de certificat :

| Option   | Description   |
|--|---|
| Générer une demande de signature de nom de domaine complet | <ul style="list-style-type: none"> <li>■ Cliquez sur <b>Générer une demande de signature de nom de domaine complet</b>, cliquez sur le bouton <b>Copier dans le Presse-papiers</b>, puis cliquez sur <b>Fermer</b>.</li> <li>■ Pour générer le certificat signé, transmettez la demande de signature de certificat à l'autorité de certification (CA).</li> <li>■ Dans la zone de texte <b>Certificat</b>, collez le certificat signé généré au format PEM et cliquez sur <b>Importer</b>.</li> </ul> |
| Générer une demande de signature d'IP                      | <ul style="list-style-type: none"> <li>■ Cliquez sur <b>Générer une demande de signature d'IP</b>, cliquez sur le bouton <b>Copier dans le Presse-papiers</b>, puis cliquez sur <b>Fermer</b>.</li> <li>■ Pour générer le certificat signé, transmettez la demande de signature de certificat à l'autorité de certification.</li> <li>■ Dans la zone de texte <b>Certificat</b>, collez le certificat signé généré au format PEM et cliquez sur <b>Importer</b>.</li> </ul>                           |

Il n'est pas nécessaire d'importer le certificat immédiatement. Pour vous assurer que vous pouvez utiliser le certificat signé, ne redémarrez pas l'hôte entre la génération de la demande de signature de certificat et l'importation du certificat.

La demande de signature de certificat est ensuite transmise à l'autorité de certification pour générer le certificat officiel.

Une demande de nom de domaine complet dispose du nom d'hôte complet de l'hôte dans le champ de nom commun résultant du certificat. La demande de signature IP a l'adresse IP de l'hôte dans le champ de nom commun.

## Gérer les utilisateurs avec VMware Host Client

Vous devez gérer les utilisateurs pour contrôler ceux qui sont autorisés à se connecter à ESXi.

Les utilisateurs et les rôles contrôlent les éléments autorisés à accéder aux composants hôtes d'ESXi et définissent les actions que chaque utilisateur peut accomplir.

Dans vSphere 5.1 et les versions ultérieures, la gestion des utilisateurs ESXi fait l'objet des mises en garde suivantes.

- Les utilisateurs qui sont créés lorsque vous vous connectez directement à un hôte ESXi ne sont pas les mêmes que ceux de vCenter Server. Lorsque l'hôte est géré par vCenter Server, vCenter Server ignore les utilisateurs créés directement sur l'hôte.
- Vous ne pouvez pas créer d'utilisateurs ESXi avec vSphere Client. Vous devez vous connecter directement à l'hôte avec VMware Host Client afin de créer des utilisateurs ESXi.
- ESXi 5.1 et versions ultérieures ne prennent pas en charge les groupes locaux. Cependant, les groupes Active Directory sont pris en charge.

Afin d'empêcher des utilisateurs anonymes, tels que racine, d'accéder à l'hôte avec l'interface utilisateur de la console directe (DCUI) ou ESXi Shell, supprimez les privilèges administrateur de l'utilisateur dans le dossier racine de l'hôte. Cela s'applique aux utilisateurs locaux ainsi qu'aux utilisateurs et aux groupes Active Directory.

## Ajouter un utilisateur ESXi dans VMware Host Client

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

### Conditions préalables

Pour plus d'informations sur les exigences en matière de mot de passe, consultez [Configurer la politique de mot de passe et de verrouillage de compte dans VMware Host Client](#) ou la documentation *Sécurité vSphere*.

### Procédure

- 1 Connectez-vous à ESXi avec VMware Host Client.  
Vous ne pouvez pas créer d'utilisateurs ESXi avec vSphere Client. Pour créer des utilisateurs ESXi, vous devez vous connecter directement à l'hôte avec VMware Host Client.
- 2 Cliquez sur **Gérer** dans l'inventaire VMware Host Client et cliquez sur **Sécurité et utilisateurs**.
- 3 Cliquez sur **Utilisateurs**.
- 4 Cliquez sur **Ajouter utilisateur**.
- 5 Entrez un nom d'utilisateur et un mot de passe.

---

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

---

- N'incluez aucun espace dans le nom d'utilisateur.
  - N'incluez aucun caractère non ASCII dans le nom d'utilisateur.
  - 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, un message d'erreur indique les exigences à respecter.
- 6 Pour activer l'accès local à ESXi Shell, cochez la case **Activer l'accès au shell**.
  - 7 Cliquez sur **Ajouter**.

## Mettre à jour un utilisateur ESXi dans VMware Host Client

Vous pouvez changer la description et le mot de passe d'un utilisateur ESXi dans VMware Host Client.

### Procédure

- 1 Cliquez sur **Gérer** dans l'inventaire VMware Host Client et cliquez sur **Sécurité et utilisateurs**.
- 2 Cliquez sur **Utilisateurs**.
- 3 Dans la liste, sélectionnez un utilisateur et cliquez sur **Modifier l'utilisateur**.
- 4 Mettez à jour les détails de l'utilisateur et cliquez sur **Enregistrer**.

## Supprimer un utilisateur local ESXi d'un hôte dans VMware Host Client

Vous pouvez supprimer un utilisateur ESXi local de l'hôte.

---

**Attention** 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.

---

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

---

### Procédure

- 1 Cliquez sur **Gérer** dans l'inventaire VMware Host Client et cliquez sur **Sécurité et utilisateurs**.
- 2 Cliquez sur **Utilisateurs**.
- 3 Sélectionnez l'utilisateur à supprimer de la liste. Cliquez sur **Supprimer utilisateur**, puis sur **Oui**.

En aucun cas ne retirez l'utilisateur racine.

## Gérer les rôles ESXi dans VMware Host Client

ESXi autorise l'accès aux objets uniquement aux utilisateurs qui disposent des autorisations appropriées. Lorsque vous affectez à l'utilisateur une autorisation pour l'objet, vous devez associer l'utilisateur à un rôle. Un rôle est un ensemble prédéfini de privilèges. Pour plus d'informations sur les privilèges, reportez-vous à la documentation *Sécurité vSphere*.

Les hôtes ESXi fournissent trois rôles par défaut, et vous ne pouvez pas modifier les privilèges qui leur sont associés. Chaque rôle par défaut suivant inclut les privilèges du rôle précédent. Par exemple, le rôle Administrateur hérite des privilèges du rôle Lecture seule. Les rôles que vous créez n'héritent aucun privilège de n'importe quel rôle par défaut.

Vous pouvez créer des rôles personnalisés à l'aide des fonctionnalités de modification de rôles dans VMware Host Client afin de créer des ensembles de privilèges correspondant à vos besoins utilisateurs. Par ailleurs, les rôles que vous créez directement sur un hôte ne sont pas accessibles dans vCenter Server. Vous pouvez utiliser ces rôles uniquement si vous ouvrez une session de l'hôte directement à partir de VMware Host Client.

---

**Note** Lorsque vous ajoutez un rôle personnalisé et que vous ne lui attribuez aucun privilège, le rôle est créé en lecture-seule avec le privilège défini par le système **System.Anonymous**, **System.View** et **System.Read**.

---

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

Vous pouvez créer des rôles d'hôte et configurer des autorisations via une connexion directe à l'hôte ESXi avec VMware Host Client.

## Ajouter un rôle dans VMware Host Client

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

### Conditions préalables

Vérifiez que vous êtes connecté en tant qu'utilisateur disposant des privilèges d'administrateur (par exemple, l'utilisateur racine ou l'utilisateur vpx).

### Procédure

- 1 Cliquez sur **Gérer** dans l'inventaire VMware Host Client et cliquez sur **Sécurité et utilisateurs**.
- 2 Cliquez sur **Rôles**.
- 3 Cliquez sur **Ajouter rôle**.
- 4 Entrez le nom du nouveau rôle.
- 5 Dans la liste, sélectionnez les privilèges à associer à ce rôle, puis cliquez sur **Ajouter**.

## Mettre à jour un rôle dans VMware Host Client

Quand vous modifiez un rôle, vous pouvez changer les privilèges sélectionnés pour ce rôle. Lorsque vous avez terminé, ces privilèges sont appliqués à n'importe quel utilisateur ou groupe auquel le rôle modifié a été attribué.

### Conditions préalables

Vérifiez que vous êtes connecté en tant qu'utilisateur disposant des privilèges d'administrateur (par exemple, l'utilisateur racine ou l'utilisateur vpx).

### Procédure

- 1 Cliquez sur **Gérer** dans l'inventaire VMware Host Client et cliquez sur **Sécurité et utilisateurs**.

- 2 Cliquez sur **Rôles**.
- 3 Dans la liste, sélectionnez un rôle et cliquez sur **Modifier le rôle**.
- 4 Mettez à jour les détails du rôle et cliquez sur **Enregistrer**.

## Supprimer un rôle dans VMware Host Client

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

---

**Attention** Vous devez comprendre comment les utilisateurs seront affectés avant de supprimer toutes les affectations ou de les substituer. Les utilisateurs ne disposant d'aucune autorisation ne peuvent pas ouvrir de session.

---

### Conditions préalables

Vérifiez que vous êtes connecté en tant qu'utilisateur disposant des privilèges d'administrateur (par exemple, l'utilisateur racine ou l'utilisateur vpx).

### Procédure

- 1 Cliquez sur **Gérer** dans l'inventaire VMware Host Client et cliquez sur **Sécurité et utilisateurs**.
- 2 Cliquez sur **Rôles**.
- 3 Sélectionnez le nom du rôle à supprimer de la liste.
- 4 Cliquez sur **Supprimer rôle**, puis sélectionnez **Supprimer uniquement si non utilisé** et cliquez sur **Oui**.

## Gérer des hôtes dans vCenter Server

Pour surveiller tous les hôtes de votre environnement virtuel à partir d'un emplacement unique et simplifier la configuration des hôtes, connectez les hôtes à un système vCenter Server.

Pour plus d'informations sur la gestion de la configuration des hôtes ESXi, reportez-vous aux documentations *Mise en réseau vSphere*, *Stockage vSphere* et *Sécurité vSphere*.

## Mettre à jour votre environnement VMware Host Client vers la dernière version

Pour déterminer si vous utilisez la dernière version de VMware Host Client, vérifiez que les VIB (bundles d'installation vSphere) sont installés dans votre environnement et examinez les informations sur la version des VIB. Vous pouvez mettre à jour votre environnement VMware Host Client en entrant une URL ou un chemin de banque de données vers un VIB ou vers le fichier `metadata.zip` dans un module de bundle hors ligne ESXi.



Si vous fournissez un fichier VIB, un VIB existant qui est installé sur votre environnement VMware Host Client est mis à jour avec le nouveau VIB.

Si vous fournissez un bundle hors ligne, vous mettez à jour l'intégralité de l'hôte ESXi vers la version décrite par le fichier `metadata.zip` du bundle. Assurez-vous que l'intégralité du bundle hors ligne est disponible via l'URL ou chargée dans la banque de données.

### Procédure

- ◆ Pour mettre à jour votre environnement vers la dernière version, effectuez les tâches suivantes :

| Tâche  | Étapes  |
|--|---|
| <b>Télécharger un VIB vers une banque de données</b>               | <ol style="list-style-type: none"> <li>Dans l'environnement VMware Host Client, cliquez sur <b>Stockage</b>.</li> <li>Sélectionnez une banque de données dans la liste et cliquez sur <b>Navigateur de banque de données</b>.</li> <li>Pour stocker le VIB, sélectionnez un répertoire et cliquez sur <b>Télécharger</b>.</li> <li>Accédez à l'emplacement du fichier et double-cliquez sur celui-ci.</li> </ol>  |
| <b>Télécharger un bundle hors ligne vers une banque de données</b> | <ol style="list-style-type: none"> <li>Téléchargez le module de bundle hors ligne ESXi.</li> <li>Chargez le module de bundle hors ligne ESXi sur l'hôte ESXi. Vous pouvez charger le module de bundle hors ligne à l'aide du <b>Navigateur de banque de données</b>, du protocole de copie sécurisée ou de WinSCP.</li> <li>Extrayez le contenu du bundle hors ligne sur l'hôte ESXi. Par exemple, connectez-vous à l'hôte à l'aide de SSH.</li> <li>Accédez au répertoire dans lequel vous avez téléchargé le bundle hors ligne.</li> <li>Extrayez le contenu à l'aide de la commande <pre>unzip</pre> </li> </ol> |
| <b>Mettre à jour votre environnement</b>                           | <ol style="list-style-type: none"> <li>Cliquez sur <b>Gérer</b> dans VMware Host Client, et cliquez sur <b>Packages</b>.</li> <li>Cliquez sur <b>Installer la mise à jour</b> et entrez l'URL ou le chemin de banque de données vers un VIB ou un fichier <code>metadata.zip</code> dans un bundle hors ligne.</li> <li>Cliquez sur <b>Mise à niveau</b>. <div> <p><b>Attention</b> Si vous mettez à jour un hôte ESXi géré par vSphere Lifecycle Manager, l'hôte peut devenir non conforme.</p> </div> </li> <li>Cliquez sur <b>Actualiser</b> pour vous assurer que la mise à jour est effectuée.</li> </ol>      |

## Impossible de se connecter depuis VMware Host Client à un hôte ESXi après la mise à niveau vers une version plus récente de ESXi

Après avoir mis à niveau votre hôte de ESXi vers une version plus récente, votre console de navigateur peut afficher un message d'erreur lorsque vous tentez d'accéder à votre hôte ESXi à l'aide de VMware Host Client, et votre connexion peut échouer.

## Problème

Après avoir mis à niveau votre hôte ESXi vers une version plus récente, la tentative d'accès à **https://host-fqdn/ui** ou **https://1.2.3.4/ui** risque de générer l'erreur suivante :

```
503 Service indisponible (Échec de la connexion au point de terminaison :
[N7Vmacore4Http16LocalServiceSpecE:0xffa014e8] _serverNamespace = /ui _isRedirect = false
_port = 8308)
```

## Cause

La modification en `/etc/vmware/rhttpproxy/endpoints.conf` demeure après la mise à niveau et entraîne le remplacement de VMware Host Client par `/ui`.

Lorsque `/ticket` est manquant dans le fichier `endpoint.conf` sur votre hôte ESXi 6.0 ou une version ultérieure, votre machine virtuelle dans le navigateur affiche le message d'erreur `Échec de la connexion` mais VMware Remote Console continue de fonctionner.

## Solution

- 1 Connectez-vous à votre hôte ESXi en utilisant SSH ou l'interpréteur de commandes ESXi.  
Si vous utilisez SSH, vous devrez peut-être commencer par activer SSH. Vous pouvez activer SSH à l'aide de DCUI.

- 2 Sauvegardez le fichier `endpoints.conf`.

```
cp /etc/vmware/rhttpproxy/endpoints.conf /tmp
```

- 3 Ouvrez le fichier `/etc/vmware/rhttpproxy/endpoints.conf` dans un éditeur et supprimez la ligne suivante.

```
/ui local 8308 redirect allow
```

- 4 Redémarrez le proxy Web inverse.

```
/etc/init.d/rhttpproxy restart
```

- 5 Accédez à VMware Host Client en utilisant le nom complet spécifié pour l'hôte dans l'URL sécurisée avec **https://host-fqdn/ui** ou une adresse IP numérique valide **https://1.2.3.4/ui**.

## Accéder à vSphere Client

Pour accéder à l'ensemble des fonctionnalités et aux fonctionnalités administratives et de dépannage avancées de l'hôte ESXi, connectez l'hôte ESXi à vCenter Server.

**Procédure**

- 1 Cliquez avec le bouton droit sur **Hôte** dans l'inventaire VMware Host Client et sélectionnez **Gérer avec vCenter Server** dans le menu déroulant.

La page de connexion vCenter Server s'ouvre dans une nouvelle fenêtre.

- 2 Entrez vos informations d'identification et cliquez sur **Connexion**.

## Déconnecter un hôte ESXi de vCenter Server avec VMware Host Client

Si vous ne souhaitez plus utiliser les fonctionnalités avancées fournies par vCenter Server pour la gestion des hôtes, ou si vCenter Server a échoué et que vous devez effectuer des opérations d'urgence sur l'hôte, vous pouvez déconnecter votre hôte ESXi de vCenter Server.

Déconnecter un hôte ESXi peut prendre plusieurs minutes.

**Procédure**

- 1 Cliquez avec le bouton droit sur **Hôte** dans l'inventaire VMware Host Client et sélectionnez **Déconnecter de vCenter Server** dans le menu contextuel.

---

**Note** La déconnexion d'un hôte informe vCenter Server que cet hôte ne répond pas.

---

- 2 Cliquez sur **Déconnecter de vCenter Server**.

## Redémarrer ou arrêter ESXi Host dans VMware Host Client

Vous pouvez mettre hors tension ou redémarrer n'importe quel hôte ESXi à l'aide de VMware Host Client. La mise hors tension d'un hôte géré le déconnecte de vCenter Server, mais ne le retire pas de l'inventaire.

**Conditions préalables**

Pour redémarrer ou arrêter un hôte, ces privilèges sont nécessaires.

- **Hôte.Configuration.Maintenance**
- **Global.Événement de journal**

Effectuez toujours les tâches suivantes avant de redémarrer ou d'arrêter un hôte :

- Mettez hors tension toutes les machines virtuelles sur l'hôte.
- Placer l'hôte en mode maintenance.

## Procédure

- 1 Cliquez avec le bouton droit sur l'hôte, sélectionnez **Arrêter l'hôte** ou **Redémarrer l'hôte**.

---

**Note** Si l'hôte n'est pas en mode de maintenance, l'arrêter ou le redémarrer n'arrête pas les machines virtuelles en cours d'exécution sur cet hôte de manière sécurisée et des données non sauvegardées pourraient être perdues. Si l'hôte fait partie d'un cluster vSAN, vous pourriez perdre l'accès aux données vSAN.

---

- 2 Cliquez sur **Arrêter** ou **Redémarrer** pour terminer cette procédure.

## Utilisation du ESXi Shell

ESXi Shell fournit des commandes de maintenance essentielles et est désactivé par défaut sur les hôtes ESXi. Vous pouvez activer l'accès local et distant au shell si nécessaire. Pour réduire le risque d'accès non autorisé, activez ESXi Shell pour le dépannage uniquement.

ESXi Shell est indépendant du mode verrouillage. Même si l'hôte s'exécute en mode verrouillage, vous pouvez toujours vous connecter à ESXi Shell si ce service est activé.

Reportez-vous à la section *Sécurité vSphere*.

Les services applicables sont les suivants.

### ESXi Shell

Activez ce service pour accéder localement à ESXi Shell.

### SSH

Activez ce service pour accéder à ESXi Shell à distance en utilisant SSH.

### Interface utilisateur de la console directe (DCUI)

Lorsque vous activez ce service en mode verrouillage, vous pouvez vous connecter localement à l'interface utilisateur de la console directe en tant qu'utilisateur racine, puis désactiver le mode verrouillage. Vous pouvez ensuite accéder à l'hôte via une connexion directe à VMware Host Client ou en activant ESXi Shell.

L'utilisateur racine et les utilisateurs disposant du rôle d'administrateur peuvent accéder à ESXi Shell. Les utilisateurs du groupe Active Directory ESX Admins reçoivent automatiquement le rôle d'Administrateur. Par défaut, seul l'utilisateur racine peut exécuter des commandes système (telles que `vmware -v`) en utilisant ESXi Shell.

---

**Note** N'activez pas ESXi Shell si vous n'avez pas réellement besoin d'un accès.

---

## Activer Secure Shell (SSH) dans VMware Host Client

Activez Secure Shell (SSH) pour accéder à ESXi Shell à distance en utilisant SSH.

**Procédure**

- 1 Pour activer ou désactiver Secure Shell (SSH), cliquez avec le bouton droit sur **Hôte** dans l'inventaire VMware Host Client.
- 2 Sélectionnez **Services** dans le menu déroulant.
- 3 Pour activer Secure Shell (SSH), sélectionnez **Activer Secure Shell (SSH)**.
- 4 Pour activer ESXi Shell, sélectionnez **Activer ESXi Shell**.

**Activer ESXi Console Shell dans VMware Host Client**

Lorsque vous activez ce service en mode verrouillage, vous pouvez vous connecter localement à l'interface utilisateur de la console directe en tant qu'utilisateur racine, puis désactiver le mode verrouillage. Vous pouvez ensuite accéder à l'hôte via une connexion directe à VMware Host Client ou en activant ESXi Shell.

**Procédure**

- 1 Pour activer ou désactiver Console Shell, cliquez avec le bouton droit sur **Hôte** dans l'inventaire VMware Host Client.
- 2 Sélectionnez **Services** dans le menu déroulant et sélectionnez **Console Shell**.
- 3 Sélectionnez la tâche à effectuer.
  - Si Console Shell est activé, cliquez sur **Désactiver** pour le désactiver.
  - Si Console Shell est désactivé, cliquez sur **Activer** pour l'activer.

**Créer un délai d'expiration pour la disponibilité d'ESXi Shell dans VMware Host Client**

ESXi Shell est désactivé par défaut. Pour renforcer la sécurité lorsque vous activez le shell, vous pouvez définir un délai de disponibilité pour ESXi Shell.

Le délai de disponibilité définit la durée pendant laquelle les connexions au shell local et distant sont autorisées, et au terme de laquelle la possibilité de se connecter via le shell est désactivée. Lorsque le délai de disponibilité expire, il reste des sessions shell existantes, mais les nouvelles sessions shell ne sont pas autorisées.

**Procédure**

- 1 Cliquez sur **Gérer** dans l'inventaire VMware Host Client.
- 2 Sous l'onglet **Système**, sélectionnez **Paramètres avancés**.
- 3 Entrez **UserVars.ESXiShellTimeOut** dans la zone de texte **Rechercher**, puis cliquez sur l'icône **Rechercher**.
- 4 Sélectionnez **UserVars.ESXiShellTimeOut** et cliquez sur **Modifier**.

La boîte de dialogue **Modifier l'option** s'ouvre.

- 5 Dans la zone de texte **Nouvelle valeur**, entrez le paramètre de délai d'expiration.  
Une valeur de zéro (0) désactive le délai d'expiration.
- 6 Cliquez sur **Enregistrer**.  
Vous devez redémarrer le service SSH et le service ESXi Shell pour que le délai d'expiration soit appliqué.
- 7 (Facultatif) Pour réinitialiser le paramètre de clé à la valeur par défaut, cliquez avec le bouton droit sur la clé appropriée dans la liste, puis sélectionnez l'option **Réinitialiser sur les paramètres par défaut**.

## Créer un délai d'expiration pour les sessions ESXi Shell inactives dans VMware Host Client

Si vous activez le shell ESXi sur un hôte, mais que vous oubliez de vous déconnecter de la session, la session inactive demeure connectée indéfiniment. La connexion restée ouverte augmente les possibilités qu'une personne obtienne un accès privilégié à l'hôte ESXi. Vous pouvez éviter cela en paramétrant un délai d'expiration des sessions inactives.

Le délai d'inactivité correspond à la période au terme de laquelle vous êtes déconnecté d'une session interactive inactive.

### Procédure

- 1 Cliquez sur **Gérer** dans l'inventaire VMware Host Client.
- 2 Dans l'onglet **Système**, cliquez **Paramètres avancés**.
- 3 Entrez `UserVars.ESXiShellInteractiveTimeout` dans la zone de texte **Rechercher**, puis cliquez sur l'icône **Rechercher**.
- 4 Sélectionnez `UserVars.ESXiShellInteractiveTimeout` et cliquez sur **Modifier**.  
La boîte de dialogue **Modifier l'option** s'ouvre.
- 5 Dans la zone de texte **Nouvelle valeur**, entrez le paramètre de délai d'expiration.  
Une valeur de zéro (0) désactive le délai d'expiration.
- 6 Cliquez sur **Enregistrer**.  
Le délai d'expiration prend effet uniquement pour les sessions récemment connectées.
- 7 (Facultatif) Pour réinitialiser le paramètre de clé à la valeur par défaut, cliquez avec le bouton droit sur la clé appropriée dans la liste, puis sélectionnez l'option **Réinitialiser sur les paramètres par défaut**.

### Résultats

Si la session est inactive, les utilisateurs sont déconnectés à l'expiration du délai d'attente.

## Mettre un hôte en mode de maintenance dans VMware Host Client

Vous placez un hôte en mode maintenance quand vous devez effectuer de la maintenance sur celui-ci, par exemple pour installer plus de mémoire. Un hôte entre ou quitte le mode maintenance uniquement suite à la demande d'un utilisateur.

L'hôte est en état d'**Entrée en mode maintenance** jusqu'à ce que toutes les machines virtuelles soit mises hors tension ou aient migré vers d'autres hôtes. Vous ne pouvez pas mettre des machines virtuelles hors tension ou migrer des machines virtuelles vers un hôte entrant en mode maintenance.

Pour placer un hôte en mode maintenance, toutes les machines virtuelles qui sont en cours d'exécution sur l'hôte doivent être mises hors tension ou migrées vers d'autres hôtes. Si vous essayez de placer un hôte ayant des machines virtuelles en cours d'exécution en mode maintenance, le DRS doit mettre hors tension ou migrer les machines virtuelles en cours d'exécution avant d'accomplir la tâche. Si le délai d'attente est atteint avant que les machines virtuelles ne soient mises hors tension ou aient migré, un message d'erreur apparaît.

Quand toutes les machines virtuelles sur l'hôte sont inactives, l'icône de l'hôte affiche **en cours de maintenance** et le panneau de résumé de l'hôte indique le nouvel état. Tant qu'il est en mode maintenance, l'hôte ne vous permet ni de déployer ni de mettre sous tension une machine virtuelle.

### Conditions préalables

Avant de placer un hôte en mode maintenance, mettez hors tension toutes les machines virtuelles en cours d'exécution sur cet hôte ou faites-les migrer vers un autre hôte manuellement ou automatiquement par DRS.

### Procédure

- ◆ Cliquez avec le bouton droit de la souris sur l'hôte et sélectionnez **Entrer en mode maintenance**.

### Résultats

L'hôte reste en mode maintenance jusqu'à ce que vous sélectionniez **Quitter le mode maintenance**.

## Gérer les autorisations dans VMware Host Client

Pour ESXi, les autorisations sont définies en tant que rôles d'accès. Ces rôles désignent les rôles attribués à un utilisateur pour différents objets, tels qu'une machine virtuelle ou un hôte ESXi. Les autorisations accordent aux utilisateurs le droit d'exercer les activités spécifiées par le rôle sur l'objet auquel le rôle est assigné.

Par exemple, pour configurer la mémoire de l'hôte, il faut accorder à l'utilisateur un rôle qui inclut le privilège **Hôte.Configuration.Configuration mémoire**. En attribuant différents rôles aux utilisateurs pour différents objets, vous pouvez contrôler les tâches que ces utilisateurs peuvent effectuer à l'aide de VMware Host Client.

Lors d'une connexion directe à un hôte avec VMware Host Client, les comptes d'utilisateur racine et vpxuser disposent des mêmes droits que tous les utilisateurs auxquels a été attribué le rôle Administrateur sur tous les objets.

Tous les autres utilisateurs ne disposent initialement d'aucune autorisation sur aucun objet. Cela signifie qu'ils ne peuvent ni afficher ces objets ni y exécuter de tâches. Un utilisateur avec des privilèges d'administrateur doit assigner des autorisations à ces utilisateurs afin de leur permettre d'effectuer des tâches.

Beaucoup de tâches exigent des autorisations sur plus d'un objet. Les règles suivantes peuvent vous aider à déterminer les rôles à attribuer aux utilisateurs afin de les autoriser à accomplir certaines tâches :

- N'importe quelle tâche qui consomme l'espace sur le disque dur, telle que la création d'un disque virtuel ou la prise d'un snapshot, exige le privilège **Banque de données.Allouer l'espace** sur la banque de données cible et le privilège d'exécuter l'opération elle-même.
- Chaque hôte et chaque cluster ont leur propre pool de ressources implicite qui contient toutes les ressources de cet hôte ou de ce cluster. Le déploiement d'une machine virtuelle directement sur un hôte ou un cluster exige le privilège **Ressource.Attribuer une machine virtuelle au pool de ressources**.

La liste des privilèges est la même pour ESXi et vCenter Server.

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

## Validation d'autorisation

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

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

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



## Attribuer des autorisations à un utilisateur pour un hôte ESXi dans VMware Host Client

Pour réaliser certaines actions sur un hôte ESXi, l'utilisateur doit disposer des autorisations associées à ce rôle particulier. Dans VMware Host Client, vous pouvez attribuer des rôles à des utilisateurs et leur octroyer les autorisations nécessaires à l'accomplissement de tâches variées sur l'hôte.

### Procédure

- 1 Cliquez avec le bouton droit de la souris sur **Hôte** dans l'inventaire VMware Host Client et cliquez sur **Autorisations**.

La fenêtre **Gérer les autorisations** s'affiche.

- 2 Cliquez sur **Ajouter utilisateur**.
- 3 Dans la zone de texte **Sélectionner un utilisateur**, sélectionnez l'utilisateur auquel attribuer un rôle.
- 4 Cliquez sur la flèche en regard de la zone de texte **Sélectionner un rôle** et sélectionnez un rôle dans la liste.
- 5 (Facultatif) Sélectionnez **Propager vers tous les enfants** ou **Ajouter en tant que groupe**.

Si vous définissez une autorisation à un niveau vCenter Server et que vous la propagez aux enfants de l'objet, cette autorisation s'applique aux centres de données, dossiers, clusters, hôtes, machines virtuelles ainsi qu'aux autres objets dans l'instance de vCenter Server.

- 6 Cliquez sur **Ajouter un utilisateur**, puis cliquez sur **Fermer**.

## Supprimer des autorisations pour un utilisateur dans VMware Host Client

La suppression d'une autorisation pour un utilisateur ne supprime pas celui-ci de la liste des utilisateurs disponibles. Elle ne supprime pas non plus le rôle de la liste d'éléments disponibles. Elle supprime la paire utilisateur et rôle de l'objet d'inventaire sélectionné.

### Procédure

- 1 Cliquez avec le bouton droit de la souris sur **Hôte** dans l'inventaire VMware Host Client et cliquez sur **Autorisations**.

La fenêtre **Gérer les autorisations** s'affiche.

- 2 Dans la liste, sélectionnez un utilisateur et cliquez sur **Supprimer utilisateur**.
- 3 Cliquez sur **Fermer**.

## Attribuer des autorisations utilisateur pour une machine virtuelle dans VMware Host Client

Attribuez un rôle à un utilisateur particulier afin de lui octroyer les autorisations d'accomplir des tâches spécifiques sur une machine virtuelle.

### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez avec le bouton droit de la souris sur une machine virtuelle de la liste et sélectionnez **Autorisations**.  
  
La fenêtre **Gérer les autorisations** s'affiche.
- 3 Cliquez sur **Ajouter utilisateur**.
- 4 Cliquez sur la flèche en regard de la zone de texte **Sélectionner un utilisateur** et sélectionnez l'utilisateur auquel attribuer un rôle.
- 5 Cliquez sur la flèche en regard de la zone de texte **Sélectionner un rôle** et sélectionnez un rôle dans la liste.
- 6 (Facultatif) Sélectionnez **Propager vers tous les enfants**.  
  
Si vous définissez une autorisation à un niveau vCenter Server et que vous la propagez aux enfants de l'objet, cette autorisation s'applique aux centres de données, dossiers, clusters, hôtes, machines virtuelles ainsi qu'aux objets similaires dans l'instance de vCenter Server.
- 7 Cliquez sur **Ajouter un utilisateur**, puis cliquez sur **Fermer**.

## Supprimer des autorisations pour une machine virtuelle dans VMware Host Client

Pour qu'un utilisateur ne puisse pas accomplir certaines tâches sur une machine virtuelle donnée, supprimez les autorisations de cet utilisateur sur cette machine.

La suppression d'une autorisation pour un utilisateur ne supprime pas celui-ci de la liste des utilisateurs disponibles. Elle ne supprime pas non plus le rôle de la liste d'éléments disponibles. Elle supprime la paire utilisateur et rôle de l'objet d'inventaire sélectionné.

### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez avec le bouton droit de la souris sur une machine virtuelle de la liste et sélectionnez **Autorisations**.  
  
La fenêtre **Gérer les autorisations** s'affiche.
- 3 Dans la liste, sélectionnez un utilisateur et cliquez sur **Supprimer utilisateur**.
- 4 Cliquez sur **Fermer**.

## Générer un bundle de support dans VMware Host Client

Vous pouvez générer un bundle de support pour l'hôte ESXi auquel vous êtes connecté. Le bundle de support contient les fichiers journaux et les informations système que vous pouvez utiliser pour diagnostiquer et résoudre des problèmes.

### Procédure

- 1 Cliquez avec le bouton droit sur **Host** dans l'inventaire VMware Host Client et sélectionnez **Générer un bundle de support** dans le menu déroulant.

Une boîte de dialogue contenant un lien permettant de télécharger le bundle s'ouvre quand le bundle de support est créé.

- 2 (Facultatif) Cliquez sur **Surveiller** dans l'inventaire VMware Host Client, cliquez sur **Tâches**, puis sur un bundle de journaux de la liste.

Vous pouvez afficher le lien vers le bundle de journaux sous le tableau.

## Mode de verrouillage dans VMware Host Client

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

### Mode de verrouillage normal et mode de verrouillage strict

Avec vSphere 6.0 et versions ultérieures, vous pouvez sélectionner le mode de verrouillage normal ou le mode de verrouillage strict.

#### Mode de verrouillage normal

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

- Comptes répertoriés dans la liste des utilisateurs exceptionnels pour le mode de verrouillage qui disposent des privilèges d'administration sur l'hôte. La liste des utilisateurs exceptionnels est destinée aux comptes de service qui exécutent des tâches spécifiques. L'ajout d'administrateurs ESXi à cette liste serait contraire à l'objectif du mode de verrouillage.
- Les utilisateurs définis dans l'option avancée DCUI.Access de l'hôte. Cette option sert d'accès de secours à l'interface utilisateur de la console directe en cas de perte de connexion avec vCenter Server. Ces utilisateurs n'ont pas besoin de disposer de privilèges d'administration sur l'hôte.

#### Mode de verrouillage strict

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

## Mode de verrouillage et services ESXi Shell et SSH

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

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

---

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

---

## Mettre un hôte ESXi en mode de verrouillage normal avec VMware Host Client

Vous pouvez utiliser VMware Host Client pour passer en mode de verrouillage normal.

### Procédure

- 1 Cliquez avec le bouton droit sur **Hôte** dans l'inventaire VMware Host Client, sélectionnez **Mode de verrouillage** dans le menu déroulant et sélectionnez **Passer en mode de verrouillage normal**.

Un message d'avertissement apparaît.

- 2 Cliquez sur **Passer en mode de verrouillage normal**.

## Mettre un hôte ESXi en mode de verrouillage strict avec VMware Host Client

Vous pouvez utiliser VMware Host Client pour passer en mode de verrouillage strict.

### Procédure

- 1 Cliquez avec le bouton droit sur **Hôte** dans l'inventaire VMware Host Client, sélectionnez **Mode de verrouillage** dans le menu déroulant et sélectionnez **Passer en mode de verrouillage strict**.

Le message d'avertissement apparaît.

- 2 Cliquez sur **Passer en mode de verrouillage strict**.

## Quitter le mode de verrouillage avec VMware Host Client

Si vous êtes entré en mode de verrouillage normal ou strict sur un hôte ESXi, vous pouvez quitter ce mode en utilisant VMware Host Client.

### Procédure

- ◆ Cliquez avec le bouton droit sur **Hôte** dans l'inventaire VMware Host Client, sélectionnez **Mode de verrouillage** dans le menu déroulant et sélectionnez **Quitter le mode de verrouillage**.

## Spécifier les utilisateurs exceptionnels du mode de verrouillage dans VMware Host Client

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

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

---

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

---

### Procédure

- 1 Cliquez sur **Gérer** dans l'inventaire VMware Host Client et cliquez sur **Sécurité et utilisateurs**.
- 2 Cliquez sur **Mode de verrouillage**.
- 3 Cliquez sur **Ajouter une exception utilisateur**, entrez le nom de l'utilisateur et cliquez sur **Ajouter une exception**.
- 4 (Facultatif) Sélectionnez un nom dans la liste des utilisateurs exceptionnels, cliquez sur **Supprimer l'exception utilisateur** et cliquez sur **Confirmer**.

## Gérer des ressources CPU à l'aide de VMware Host Client

Lorsque vous vous connectez à un hôte ESXi avec VMware Host Client, vous avez accès à un nombre limité de paramètres de gestion des ressources.

## Afficher les informations sur les processeurs en utilisant VMware Host Client

Dans VMware Host Client, vous pouvez accéder aux informations sur la configuration actuelle des CPU de l'hôte ESXi auquel vous êtes connecté.

### Procédure

- 1 Cliquez sur **Hôte** dans l'inventaire VMware Host Client.
- 2 Développez **Matériel** et développez **CPU**.

Vous pouvez afficher les informations relatives au numéro et au type des processeurs physiques ainsi que le nombre de processeurs logiques.

## Attribuer une machine virtuelle à un processeur spécifique dans VMware Host Client

Avec l'affinité de CPU, vous pouvez attribuer une machine virtuelle à un processeur spécifique. De cette façon, vous ne pouvez attribuer une machine virtuelle qu'à un processeur disponible spécifique dans les systèmes multiprocesseurs.

### Conditions préalables

Mettez la machine virtuelle hors tension.

### Procédure

- 1 Cliquez avec le bouton droit de la souris sur la machine virtuelle dans l'inventaire VMware Host Client et sélectionnez **Modifier les paramètres**.
- 2 Sous **Matériel virtuel**, développez **CPU**.
- 3 Sous **Affinité de planification**, sélectionnez l'affinité de processeur physique pour la machine virtuelle.

Utilisez un trait d'union pour indiquer les plages et une virgule pour séparer les valeurs.

Par exemple, **0, 2, 4-7** fait référence aux processeurs 0, 2, 4, 5, 6 et 7.

- 4 Cliquez sur **Enregistrer** pour appliquer vos modifications.

## Surveiller un hôte ESXi dans VMware Host Client

Lorsque vous vous connectez à un hôte avec VMware Host Client, vous pouvez surveiller l'état de santé de l'hôte et afficher les graphiques de performances, les événements, les tâches, les journaux système et les notifications.

## Afficher les graphiques dans VMware Host Client

Lorsque vous êtes connecté à VMware Host Client, vous pouvez afficher les informations sur l'utilisation des ressources de l'hôte ESXi que vous gérez sous la forme d'un graphique linéaire.

Pour réduire la consommation de la mémoire, VMware Host Client contient uniquement les statistiques de la dernière heure.

#### Procédure

- 1 Cliquez sur **Surveiller** dans VMware Host Client et cliquez sur **Performance**.
- 2 (Facultatif) Pour afficher l'utilisation de l'hôte au cours de la dernière heure, sélectionnez une option dans le menu déroulant.
  - Pour afficher le pourcentage de CPU que l'hôte a utilisé au cours de la dernière heure, sélectionnez **CPU**.
  - Pour afficher le pourcentage de mémoire que l'hôte a utilisé au cours de la dernière heure, sélectionnez **Mémoire**.
  - ◆ Pour afficher le pourcentage de réseau que l'hôte a consommé pendant la dernière heure, sélectionnez **Réseau**.
  - ◆ Pour afficher l'utilisation de disque que l'hôte a consommé pendant la dernière heure, sélectionnez **Disque**.

## Surveiller l'état de santé du matériel dans VMware Host Client

Lorsque vous êtes connecté au VMware Host Client, vous pouvez surveiller l'état de santé du matériel de l'hôte ESXi.

---

**Note** L'état de santé du matériel est uniquement disponible quand le matériel sous-jacent le prend en charge.

---

#### Procédure

- 1 Cliquez sur **Surveiller** dans l'inventaire VMware Host Client et cliquez sur **Matériel**.
- 2 Sélectionnez le type d'informations à afficher.
- 3 (Facultatif) Utilisez les contrôles de filtre sous la liste pour filtrer la liste.
- 4 (Facultatif) Cliquez sur l'en-tête d'une colonne pour trier la liste.

## Afficher les événements dans VMware Host Client

Les événements sont des enregistrements des actions des utilisateurs ou des actions du système qui ont lieu sur un hôte ESXi. Lorsque vous êtes connecté à VMware Host Client, vous pouvez afficher tous les événements associés à l'hôte que vous gérez.

#### Conditions préalables

Privilège nécessaire : **Lecture seule**.

**Procédure**

- ◆ Cliquez sur **Surveiller** dans l'inventaire VMware Host Client et cliquez sur **Événements**.
  - a (Facultatif) Sélectionnez un événement pour afficher les détails.
  - b (Facultatif) Utilisez les contrôles de filtre sous la liste pour filtrer la liste.
  - c (Facultatif) Cliquez sur l'en-tête d'une colonne pour trier la liste.

## Afficher les tâches dans VMware Host Client

Lorsque vous êtes connecté à VMware Host Client, vous pouvez afficher les tâches qui sont associées à l'hôte ESXi. Vous pouvez afficher des informations sur l'initiateur des tâches, l'état des tâches, le résultat des tâches, la description des tâches, etc.

**Procédure**

- ◆ Cliquez sur **Surveiller** dans l'inventaire VMware Host Client et cliquez sur **Tâches**.
  - a (Facultatif) Sélectionnez une tâche pour afficher les détails.
  - b (Facultatif) Utilisez les contrôles de filtre sous la liste pour filtrer la liste.
  - c (Facultatif) Cliquez sur l'en-tête d'une colonne pour trier la liste.

## Afficher les journaux système dans VMware Host Client

Lorsque vous êtes connecté à un hôte ESXi avec VMware Host Client, vous pouvez afficher les entrées des journaux pour obtenir des informations telles que l'auteur d'un événement, la date de création de l'événement et le type de l'événement.

**Procédure**

- 1 Cliquez sur **Surveiller** dans l'inventaire VMware Host Client et cliquez sur **Journaux**.  
La liste des journaux apparaît.
- 2 (Facultatif) Cliquez sur un journal pour afficher ses détails.
- 3 (Facultatif) Cliquez avec le bouton droit sur un journal et sélectionnez l'une des options suivantes :
  - **Ouvrir une nouvelle fenêtre**
  - **Générer un bundle de support**

## Afficher les notifications dans VMware Host Client

Lorsque vous êtes connecté à VMware Host Client, vous pouvez afficher les notifications et les recommandations de l'hôte sur les tâches associées que vous devriez effectuer.

**Procédure**

- 1 Cliquez sur **Surveiller** dans l'inventaire VMware Host Client et cliquez sur **Notifications**.



**2** Sélectionnez une notification dans la liste pour afficher l'action recommandée.

Un message avec une action recommandée et une description apparaît dans la liste des notifications.

# Gestion des machines virtuelles avec VMware Host Client

# 4

Les machines virtuelles peuvent être configurées comme des ordinateurs physiques et peuvent effectuer les mêmes tâches. Les machines virtuelles prennent également en charge des fonctionnalités spécifiques non assurées par les ordinateurs physiques.

Vous pouvez utiliser VMware Host Client pour créer, enregistrer et gérer des machines virtuelles et pour effectuer des tâches administratives et de dépannage quotidiennes.

Ce chapitre contient les rubriques suivantes :

- [Créer une machine virtuelle dans VMware Host Client](#)
- [Enregistrer une machine virtuelle existante dans VMware Host Client](#)
- [Utiliser les consoles dans VMware Host Client](#)
- [Gérer un système d'exploitation invité dans VMware Host Client](#)
- [Présentation de VMware Tools](#)
- [Configuration d'une machine virtuelle dans VMware Host Client](#)
- [Gérer des machines virtuelles dans VMware Host Client](#)
- [Gérer des machines virtuelles avec des snapshots](#)
- [Surveiller une machine virtuelle dans VMware Host Client](#)

## Créer une machine virtuelle dans VMware Host Client

Les machines virtuelles sont l'élément clé dans une infrastructure virtuelle. Vous pouvez créer des machines virtuelles à ajouter à l'inventaire d'hôte. Lorsque vous créez une machine virtuelle, vous l'associez à une banque de données spécifique et vous sélectionnez un système d'exploitation et des options de matériel virtuel. Une fois la machine virtuelle sous tension, elle consomme des ressources dynamiquement à mesure que la charge de travail augmente, ou elle renvoie des ressources dynamiquement pendant que la charge de travail diminue.

Chaque machine virtuelle a les périphériques virtuels qui jouent le même rôle que le matériel physique. Une machine virtuelle obtient la CPU et mémoire, l'accès au stockage, et la connexion réseau du hôte qu'elle exécute en fonction.

## Conditions préalables

Vérifiez que vous disposez des privilèges **Machine virtuelle.Inventaire.Créer**.

En fonction des propriétés de la machine virtuelle que vous souhaitez créer, vous pouvez avoir besoin de privilèges supplémentaires.

- **Machine virtuelle.Configurer.Ajouter un disque existant** si vous incluez un périphérique de disque virtuel qui fait référence à un fichier de disque virtuel existant (pas RDM).
- **Machine virtuelle.Configurer.Ajouter un nouveau disque** si vous incluez un périphérique de disque virtuel qui crée un nouveau fichier de disque virtuel (pas RDM).
- **Machine virtuelle.Configurer.Périphérique brut** si vous incluez un mappage de périphérique brut (RDM) ou un périphérique de relais SCSI.
- **Machine virtuelle.Configurer.Périphérique USB hôte** si vous incluez un périphérique VirtualUSB répondant d'un périphérique USB hôte.
- **Machine virtuelle.Configurer.Configuration avancée** si vous définissez des valeurs dans `ConfigSpec.extraConfig`.
- **Machine virtuelle.Configurer.Remplacer placement** si vous définissez `swapPlacement`.
- **Banque de données.Allouer de l'espace** requis sur toutes les banques de données où la machine virtuelle et ses disques virtuels sont créés.
- **Réseau.Attribuer** requis sur le réseau qui est attribué à la nouvelle machine virtuelle qui est créée.

## Procédure

- 1 Cliquez avec le bouton droit sur **Hôte** dans l'inventaire VMware Host Client et sélectionnez **Créer/Enregistrer VM**.

L'assistant **Nouvelle machine virtuelle** s'ouvre.

- 2 Sélectionnez **Créer une nouvelle machine virtuelle** et cliquez sur **Suivant**.
- 3 Sur la page **Sélectionner un nom et un système d'exploitation invité**, fournissez un nom unique pour la machine virtuelle et configurez le système d'exploitation invité.
  - a Dans la zone de texte **Nom**, entrez le nom de la machine virtuelle.
  - b Dans le menu déroulant **Compatibilité**, sélectionnez la compatibilité de la machine virtuelle.
  - c Dans le menu déroulant **Famille de SE invité**, sélectionnez le système d'exploitation invité.

- d Dans le menu déroulant **Version du SE invité**, sélectionnez la version du système d'exploitation invité.
- e Pour activer VBS sur la machine virtuelle, cochez la case **Activer la sécurité basée sur la virtualisation Windows** et cliquez sur **Suivant**.

---

**Note** L'option **Activer la sécurité basée sur la virtualisation de Windows** ne s'affiche que pour les dernières versions du système d'exploitation Windows, par exemple Windows 10 et Windows Server 2016, et si la compatibilité de la machine virtuelle est ESXi 6.7 et versions ultérieures.

---

Lorsque vous activez cette option, la virtualisation matérielle, IOMMU, EFI et le démarrage sécurisé sont disponibles pour le système d'exploitation invité. Vous devez également activer la **Sécurité basée sur la virtualisation** dans le système d'exploitation invité de cette machine virtuelle.

- 4 Cliquez sur **Suivant**.
- 5 Sur la page **Sélectionner le stockage**, sélectionnez le type de stockage de la machine virtuelle et une banque de données dans laquelle stocker les fichiers de la machine virtuelle.
  - a Cliquez sur le bouton **Standard** pour enregistrer tous les disques de machine virtuelle et fichiers de configuration sur une banque de données standard.
  - b Pour enregistrer les disques durs de la machine virtuelle sur la banque de données PMem locale de l'hôte, cliquez sur le bouton **Mémoire persistante**.
  - c Sélectionnez une banque de données dans la liste et cliquez sur **Suivant**.

---

**Note** Vous ne pouvez pas stocker les fichiers de configuration sur une banque de données PMem. Si vous choisissez d'utiliser PMem, vous devez sélectionner une banque de données standard pour les fichiers de configuration de la machine virtuelle.

---

- 6 Sur la page **Personnaliser les paramètres**, configurez le matériel et les options de la machine virtuelle et cliquez sur **Suivant**.

Pour obtenir des informations sur les options des machines virtuelles et sur la configuration des disques virtuels, y compris des instructions pour ajouter différents types de périphériques, reportez-vous à *Administration d'une machine virtuelle vSphere*.

- a Sur la page **Personnaliser les paramètres**, cliquez sur **Matériel virtuel** et ajoutez un nouveau périphérique matériel virtuel.
- Cliquez sur l'icône **Ajouter un disque dur** pour ajouter un nouveau disque dur virtuel.

---

**Note** Vous pouvez ajouter un disque dur à mémoire persistante ou standard à la machine virtuelle. Le disque dur à mémoire persistante est stocké sur la banque de données PMem locale au niveau de l'hôte.

---

- Cliquez sur l'icône **Ajouter un adaptateur réseau** pour ajouter une carte réseau à la machine virtuelle.
- Cliquez sur l'icône **Ajouter un autre périphérique** afin de choisir un autre type de périphérique à ajouter à la machine virtuelle.

---

**Note** Si la machine virtuelle utilise le stockage PMem, les disques durs qui sont stockés sur une banque de données PMem et les périphériques NVDIMM que vous ajoutez à la machine virtuelle partagent tous les mêmes ressources PMem. Par conséquent, vous devez ajuster la taille des périphériques récemment ajoutés en fonction de la quantité de PMem disponible pour l'hôte. Si une partie de la configuration nécessite une attention, l'assistant vous en avertit.

---

- b (Facultatif) Pour afficher et configurer les paramètres du périphérique, développez n'importe quel périphérique.

| Option  | Description  |
|---------|--|
| CPU     | La CPU, ou processeur, est, dans un ordinateur, le composant qui exécute les instructions d'un logiciel et constitue l'élément principal effectuant les fonctions de l'ordinateur. Les CPU contiennent des cœurs. Le nombre de CPU virtuels disponibles pour une machine virtuelle dépend du nombre de CPU sous licence sur l'hôte et du nombre de CPU pris en charge par le système d'exploitation invité. Pour pouvoir utiliser la fonctionnalité de CPU virtuels multicœurs VMware, vous devez respecter les conditions de CLUF du système d'exploitation invité.   |
| Mémoire | Vous pouvez ajouter, modifier ou configurer des ressources ou des options de mémoire de machine virtuelle pour améliorer les performances de machine virtuelle. Vous pouvez définir la plupart des paramètres de mémoire pendant la création de machine virtuelle ou après avoir installé le système d'exploitation client. Les paramètres des ressources de mémoire d'une machine virtuelle déterminent la quantité de mémoire de l'hôte allouée à la machine virtuelle. La taille de la mémoire du matériel virtuel détermine la quantité de mémoire disponible pour les applications qui s'exécutent dans la machine virtuelle. |

| Option                            | Description   |
|-----------------------------------|---|
| <b>Disque dur</b>                 | Vous pouvez ajouter des disques virtuels haute capacité aux machines virtuelles et ajouter de l'espace aux disques existants, même lorsque la machine virtuelle est en cours d'exécution. Vous pouvez définir la plupart des paramètres de disque virtuel pendant la création de machine virtuelle ou après avoir installé le système d'exploitation invité.  |
| <b>Contrôleur SCSI</b>            | Les contrôleurs virtuels apparaissent sur une machine virtuelle comme différents types de contrôleurs SCSI, y compris BusLogic Parallel, LSI Logic Parallel, LSI Logic SAS et VMware Paravirtual SCSI. Vous pouvez définir le type de partage de bus SCSI pour une machine virtuelle et indiquer si le bus SCSI est partagé. Selon le type de partage, les machines virtuelles peuvent accéder en même temps au même disque virtuel sur le même serveur ou sur n'importe quel serveur. Vous pouvez changer la configuration de contrôleur SCSI d'une machine virtuelle sur un hôte ESXi uniquement.   |
| <b>Contrôleur SATA</b>            | Si une machine virtuelle possède plusieurs disques durs ou périphériques CD/DVD-ROM, vous pouvez ajouter jusqu'à trois contrôleurs SATA supplémentaires auxquels affecter les périphériques. Lorsque vous répartissez les périphériques entre plusieurs contrôleurs, vous pouvez améliorer les performances et éviter la congestion du trafic de données. Vous pouvez également ajouter des contrôleurs supplémentaires si vous dépassez la limite de 30 périphériques pour un seul contrôleur. Vous pouvez démarrer des machines virtuelles à partir des contrôleurs SATA et les utiliser pour des disques durs virtuels de grande capacité. |
| <b>Adaptateur réseau</b>          | <p>Quand vous configurez une machine virtuelle, vous pouvez ajouter des adaptateurs réseau et spécifier le type d'adaptateur. Les types d'adaptateurs réseau qui sont disponibles dépendent des facteurs suivants :</p> <ul style="list-style-type: none"> <li>■ La compatibilité de la machine virtuelle, qui dépend de l'hôte qui l'a créée ou récemment mise à niveau.</li> <li>■ Si la compatibilité de la machine virtuelle a été mise à niveau avec la version la plus récente de l'hôte actuel.</li> <li>■ Le système d'exploitation client.</li> </ul>  |
| <b>Lecteur de CD/DVD</b>          | Vous pouvez configurer les périphériques DVD ou CD pour vous connecter aux périphériques de client, aux périphériques d'hôte ou aux fichiers ISO de la banque de données.   |
| <b>Carte vidéo</b>                | Vous pouvez sélectionner les paramètres par défaut ou spécifier des paramètres personnalisés. Vous pouvez spécifier le nombre d'écrans, la mémoire vidéo totale et activer la prise en charge 3D pour les systèmes d'exploitation invités sur lesquels VMware prend en charge la 3D.  |
| <b>périphérique PCI</b>           | Vous pouvez configurer des périphériques PCI sur un hôte ESXi afin de les rendre disponibles pour le relais. Vous pouvez également modifier l'étiquette de matériel afin de limiter le placement des machines virtuelles à des instances matérielles spécifiques.   |
| <b>Périphérique PCI dynamique</b> | Les périphériques de relais PCI sont automatiquement regroupés selon leur fournisseur et leur nom de modèle. Vous pouvez configurer les périphériques souhaités selon le fournisseur et le nom du modèle au lieu de sélectionner un périphérique PCI physique selon l'adresse matérielle. Vous pouvez ajouter tous les périphériques disponibles avec la même étiquette de matériel ou une étiquette de matériel vide à une machine   |

| Option                           | Description  |
|----------------------------------|--|
|                                  | virtuelle. Lorsque vous mettez sous tension une machine virtuelle, des périphériques de relais PCI physiques spécifiques avec des noms de fournisseur et de modèle correspondants sont attachés à la machine virtuelle.  |
| <b>Périphériques de sécurité</b> | Vous pouvez configurer des extensions vSGX (Virtual Intel® Software Guard Extensions) pour les machines virtuelles et fournir une sécurité supplémentaire à vos charges de travail. Vous pouvez activer ou désactiver vSGX lorsque vous créez une machine virtuelle ou modifiez une machine virtuelle existante. |

- c (Facultatif) Pour supprimer un périphérique, cliquez sur l'icône de suppression (🗑️) en regard du périphérique.

Cette option apparaît uniquement pour le matériel virtuel que vous pouvez supprimer en toute sécurité.

- d (Facultatif) Pour personnaliser les options de la machine virtuelle, cliquez sur le bouton **Options de VM**.

7 Sur la page **Prêt à terminer**, passez en revue les détails et cliquez sur **Terminer**.

## Enregistrer une machine virtuelle existante dans VMware Host Client

Si vous annulez l'enregistrement d'une machine virtuelle d'un hôte sans la supprimer de la banque de données, vous pouvez réenregistrer la machine virtuelle à l'aide de VMware Host Client. Après le réenregistrement d'une machine virtuelle, celle-ci figure dans l'inventaire.

Utilisez le navigateur de banque de données pour sélectionner une banque de données, un répertoire ou un fichier `.vmtx` à ajouter à la liste des machines virtuelles que vous enregistrez. La sélection d'une banque de données ou d'un répertoire recherche tous les fichiers `.vmtx` à cet emplacement. Vous pouvez explorer plusieurs fois pour ajouter des machines virtuelles à la liste.

### Procédure

- 1 Cliquez avec le bouton droit sur **Hôte** dans l'inventaire VMware Host Client et sélectionnez **Créer/Enregistrer VM**.  
L'assistant **Nouvelle machine virtuelle** s'ouvre.
- 2 Sur la page **Sélectionner un type de création**, sélectionnez **Enregistrer une machine virtuelle existante** et cliquez sur **Suivant**.
- 3 Sur la page **Sélectionner des VM à enregistrer**, cliquez sur **Sélectionnez une ou plusieurs machines virtuelles, une banque de données ou un répertoire**, localisez la machine virtuelle que vous souhaitez enregistrer, puis cliquez sur **Sélectionner**.
- 4 Pour supprimer une machine virtuelle de la liste, sélectionnez le nom du fichier et cliquez sur **Supprimer la sélection**.

- 5 Pour annuler la sélection et recommencer, cliquez sur **Supprimer tous**.
- 6 Cliquez sur **Suivant**.
- 7 Sur la page **Prêt à terminer**, passez en revue les détails et cliquez sur **Terminer**.

## Utiliser les consoles dans VMware Host Client

Vous pouvez accéder à une machine virtuelle via une console de navigateur ou via VMware Remote Console (VMRC) dans VMware Host Client et effectuer différentes tâches sur la machine virtuelle.

### Utilisation de la console du navigateur

---

**Note** La console du navigateur n'est pas prise en charge pour les versions antérieures à 6.0 de ESXi. Vous devez utiliser VMRC afin d'accéder à la console du navigateur.

---

Vous pouvez utiliser une console de navigateur pour accéder au système d'exploitation invité sans installer de logiciel supplémentaire. Pour des fonctionnalités de console supplémentaires, comme associer du matériel local, installez VMware Remote Console.

---

**Note** Pour le moment, les consoles de navigateur prennent uniquement en charge les dispositions de clavier américaine, japonaise et allemande. Sélectionnez la disposition de clavier désirée avant d'ouvrir la console.

---

### Utilisation de VMware Remote Console

VMware Remote Console fournit un accès aux machines virtuelles sur les hôtes distants et effectue des opérations de console et de périphériques comme la configuration des paramètres des systèmes d'exploitation et la surveillance de la console de machine virtuelle pour *VMware vSphere*. Vous pouvez effectuer de nombreuses tâches sur la machine virtuelle, comme le redémarrage et la mise hors tension du système d'exploitation invité, la reprise et l'interruption de la machine virtuelle, la configuration des mises à jour de VMware Tools, la configuration et la gestion de la machine virtuelle et des différents périphériques, etc. VMRC peut également modifier les paramètres des machines virtuelles comme la RAM, les cœurs de CPU et les disques. VMware Workstation™, VMware Fusion™ ou VMware Player™ fonctionnent en tant que clients VMRC afin que vous n'ayez pas à télécharger et à installer VMRC si l'un des trois est installé sur votre système.

Pour un ensemble complet de fonctionnalités de console, vous pouvez télécharger et installer VMRC.

### Installer l'application VMware Remote Console dans VMware Host Client

VMware Remote Console (VMRC) est une application de console autonome qui permet de connecter des périphériques clients et de lancer des consoles de machines virtuelles sur des hôtes distants.



### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.  
La liste des machines virtuelles disponibles sur l'hôte s'affiche.
- 2 Sélectionnez une machine virtuelle dans la liste.
- 3 Cliquez sur l'icône **Console** de la barre d'outils et sélectionnez l'option **Télécharger VMRC**.

## Lancer la console distante pour une machine virtuelle dans VMware Host Client

Vous pouvez accéder aux machines virtuelles dans VMware Host Client avec VMware Remote Console. Vous pouvez lancer une ou plusieurs consoles pour accéder à plusieurs machines virtuelles distantes à la fois.

### Conditions préalables

Vérifiez que VMware Remote Console est installé sur votre système local.

### Procédure

- 1 Cliquez sur **Machine virtuelle** dans l'inventaire VMware Host Client et cliquez sur une machine virtuelle dans la liste.
- 2 Cliquez sur **Console** et sélectionnez **Lancer une console distante** dans le menu déroulant.  
VMware Remote Console s'ouvre en tant qu'application autonome pour la machine virtuelle sélectionnée.

## Ouvrir une console de machine virtuelle dans VMware Host Client

Avec VMware Host Client, vous pouvez accéder au bureau d'une machine virtuelle en lançant une console sur la machine virtuelle. Depuis la console, vous pouvez exécuter des tâches dans la machine virtuelle, telles que configurer les paramètres du système d'exploitation, exécuter des applications, contrôler les performances, etc.

### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Sélectionnez une machine virtuelle sous tension dans la liste.
- 3 Cliquez sur l'icône **Console** dans la barre d'outils et indiquez si vous voulez ouvrir la console dans une fenêtre contextuelle, une nouvelle fenêtre ou un nouvel onglet.

## Gérer un système d'exploitation invité dans VMware Host Client

Avec VMware Host Client, vous pouvez gérer le système d'exploitation invité de la machine virtuelle. Vous pouvez installer et mettre à jour VMware Tools et vous pouvez également arrêter, redémarrer et modifier le système d'exploitation invité configuré.

### Arrêter et redémarrer un système d'exploitation invité en utilisant VMware Host Client

Installez VMware Tools sur une machine virtuelle pour pouvoir arrêter et redémarrer le système d'exploitation invité sur cette machine virtuelle.

#### Procédure

- ◆ Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client, sélectionnez une machine virtuelle, puis sélectionnez votre tâche.
  - Pour arrêter une machine virtuelle, cliquez dessus avec le bouton droit et sélectionnez **SE invité > Arrêter**.
  - Pour redémarrer une machine virtuelle, cliquez avec le bouton de la souris sur la machine virtuelle et sélectionnez **SE invité > Redémarrer**.

### Changer le système d'exploitation invité dans VMware Host Client

Lorsque vous changez le type de système d'exploitation invité dans les paramètres des machines virtuelles, vous changez le paramètre du système d'exploitation invité dans le fichier de configuration de la machine virtuelle. Pour changer le système d'exploitation invité, vous devez installer le nouveau système d'exploitation dans la machine virtuelle.

Quand vous définissez le type de système d'exploitation invité d'une nouvelle machine virtuelle, vCenter Server applique les valeurs de configuration par défaut selon le type du système d'exploitation invité. La modification du paramètre du type du système d'exploitation invité affecte les plages et recommandations disponibles des paramètres des machines virtuelles.

#### Conditions préalables

Mettez la machine virtuelle hors tension.

#### Procédure

- 1 Dans l'inventaire VMware Host Client, cliquez avec le bouton droit sur la machine virtuelle et choisissez **Modifier les paramètres**.
- 2 Cliquez sur l'onglet **Options VM** et développez **Options générales**.

### 3 Sélectionnez un type et une version de système d'exploitation invité.

Si vous choisissez une version de système d'exploitation Windows qui prend en charge VBS et si la compatibilité de la machine virtuelle est ESXi 6.7 et versions ultérieures, la ligne VBS apparaît désormais sur l'onglet **Options VM**.

### 4 (Facultatif) Cliquez sur **Activer la sécurité basée sur la virtualisation** pour activer VBS.

---

**Important** L'activation de VBS requiert que vous utilisiez EFI pour démarrer la machine virtuelle. Modifier le microprogramme peut empêcher le SE invité de démarrer.

---

### 5 Cliquez sur **Enregistrer** pour appliquer vos modifications.

#### Résultats

Les paramètres de configuration de la machine virtuelle pour le système d'exploitation invité sont changés. Vous pouvez désormais installer le système d'exploitation client.

## Présentation de VMware Tools

VMware Tools est un ensemble de services et de modules qui activent plusieurs fonctionnalités dans les produits VMware pour une meilleure gestion des systèmes d'exploitation invités et des interactions utilisateurs plus transparente avec eux.

VMware Tools peut :

- Transmettre des messages du système d'exploitation hôte vers le système d'exploitation invité.
- Personnaliser des systèmes d'exploitation invités dans le cadre de vCenter Server et d'autres produits VMware.
- Exécuter des scripts qui facilitent l'automatisation des opérations du système d'exploitation invité. Les scripts s'exécutent lorsque l'état d'alimentation de la machine virtuelle change.
- Synchroniser l'heure du système d'exploitation invité avec celle du système d'exploitation hôte.

VMware Tools Lifecycle Management fournit une approche simplifiée et évolutive pour l'installation et la mise à niveau de VMware Tools. Il contient des améliorations des fonctionnalités et des pilotes et la prise en charge de nouveaux systèmes d'exploitation invités.

Vous devez exécuter la dernière version de VMware Tools ou utiliser open-vm-tools distribué avec la distribution Linux OS. Bien qu'un système d'exploitation invité puisse s'exécuter sans VMware Tools, vous devez toujours exécuter la dernière version de VMware Tools dans vos systèmes d'exploitation invités pour accéder aux dernières fonctionnalités et mises à jour.

Vous pouvez configurer votre machine virtuelle pour qu'elle vérifie et applique automatiquement les mises à niveau de VMware Tools à chaque fois que vous la mettez sous tension.

Pour plus d'informations sur l'activation de la mise à niveau automatique de VMware Tools sur vos machines virtuelles, consultez le *Guide d'administration d'une machine virtuelle vSphere*

## Installation de VMware Tools

Bien qu'il soit possible d'utiliser des systèmes d'exploitation invités sans VMware Tools, beaucoup de fonctionnalités VMware ne sont pas disponibles tant que vous n'installez pas VMware Tools. VMware Tools améliore les performances du système d'exploitation invité de vos machines virtuelles.

L'installation de VMware Tools fait partie du processus de création de nouvelles machines virtuelles. Il est important de mettre à niveau VMware Tools dès que les mises à jour sont disponibles. Pour plus d'informations sur la création de machines virtuelles, reportez-vous au *Guide de l'utilisateur de VMware Tools*.

Les programmes d'installation de VMware Tools sont des fichiers images ISO. Un fichier image ISO correspond à un CD-ROM physique pour le système d'exploitation client. Chaque type de système d'exploitation client, notamment Windows, Linux, Solaris, FreeBSD et NetWare, dispose d'un fichier image ISO. Lorsque vous installez ou mettez à niveau VMware Tools, le premier lecteur de CD-ROM virtuel de la machine virtuelle se connecte temporairement au fichier ISO VMware Tools du système d'exploitation client.

Pour plus d'informations sur l'installation ou la mise à niveau de VMware Tools sur des machines virtuelles Windows, Linux, Mac OS X, Solaris, NetWare ou FreeBSD, reportez-vous au *Guide de l'utilisateur de VMware Tools*.

## Installer VMware Tools à partir d'VMware Host Client

VMware Tools est une suite d'utilitaires que vous installez dans le système d'exploitation d'une machine virtuelle. VMware Tools améliore les performances et la gestion de la machine virtuelle.

Vous pouvez installer VMware Tools sur une ou plusieurs machines virtuelles à l'aide de VMware Host Client.

### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Sélectionnez une machine virtuelle dans la liste.  
La machine virtuelle doit être sous tension pour installer VMware Tools.
- 3 Cliquez sur **Actions**, sélectionnez **SE invité** dans le menu déroulant, puis sélectionnez **Installer VMware Tools**.

## Mise à niveau de VMware Tools

Vous pouvez mettre à niveau manuellement VMware Tools ou configurer les machines virtuelles pour qu'elles recherchent les versions les plus récentes de VMware Tools et les installent.

Le système d'exploitation invité vérifie la version de VMware Tools lorsque vous mettez sous tension une machine virtuelle. La barre d'état de votre machine virtuelle affiche un message lorsqu'une nouvelle version est disponible.

Pour les machines virtuelles vSphere, lorsque la version installée de VMware Tools est obsolète, la barre d'état affiche le message suivant :

Une version plus récente de VMware Tools est disponible pour cette machine virtuelle

Dans les machines virtuelles Windows, vous pouvez configurer VMware Tools pour qu'il vous signale qu'une mise à niveau est disponible. Si cette option de notification est activée, l'icône VMware Tools dans la barre des tâches Windows contient une icône jaune attention lorsqu'une mise à niveau VMware Tools est disponible.

Pour installer une mise à niveau VMware Tools, vous pouvez utiliser la même procédure que vous avez suivie pour installer VMware Tools pour la première fois. La mise à niveau de VMware Tools implique d'installer une nouvelle version.

Pour les systèmes d'exploitation clients Windows et Linux, vous pouvez configurer la machine virtuelle pour qu'elle mette à niveau automatiquement VMware Tools. Bien que la vérification de version soit effectuée lors de la mise sous tension de la machine virtuelle, sur les systèmes d'exploitation invités Windows, la mise à niveau automatique a lieu lorsque vous mettez la machine virtuelle hors tension ou la redémarrez. La barre d'état affiche le message *Installation de VMware Tools...* lorsqu'une mise à niveau est en cours. La procédure est indiquée ci-dessous.

---

**Note** La mise à niveau de VMware Tools sur les systèmes d'exploitation invités Windows installe automatiquement le pilote graphique WDDM. Le pilote graphique WDDM rend le mode veille disponible dans les paramètres d'alimentation du SE invité afin d'ajuster les options de mise en veille. Par exemple, vous pouvez utiliser le paramètre du mode veille **Modifier les conditions de mise en veille de l'ordinateur** pour configurer le SE invité pour passer automatiquement en mode veille après un certain temps ou empêcher votre SE invité de passer automatiquement en veille après un certain temps d'inactivité.

---

Pour les machines virtuelles vSphere, vous pouvez utiliser l'un des processus suivants pour mettre à niveau plusieurs machines virtuelles en même temps.

Vous pouvez utiliser l'un des processus suivants pour mettre à niveau plusieurs machines virtuelles en même temps.

- Connectez-vous à vCenter Server, sélectionnez un hôte ou un cluster, puis, dans l'onglet **Machines virtuelles**, spécifiez les machines virtuelles sur lesquelles vous souhaitez effectuer une mise à niveau de VMware Tools.
- Utilisez vSphere Lifecycle Manager pour exécuter une mise à niveau orchestrée des machines virtuelles au niveau du dossier ou du centre de données.

Des fonctions d'une version particulière d'un produit VMware peuvent dépendre de l'installation ou de la mise à niveau vers la version de VMware Tools incluse dans cette version. La mise à niveau de VMware Tools vers la dernière version n'est pas toujours nécessaire, mais elle est vivement recommandée. Les nouvelles versions de VMware Tools sont compatibles avec plusieurs versions d'hôte ESXi. Pour éviter les mises à niveau inutiles, évaluez si les fonctions

et les capacités ajoutées sont nécessaires pour votre environnement. Reportez-vous à la section [Fonctionnalités matérielles disponibles avec les paramètres de compatibilité de la machine virtuelle](#). Toutefois, VMware recommande vivement d'installer et d'utiliser la dernière version de VMware Tools.

Des fonctions d'une version particulière d'un produit VMware peuvent dépendre de l'installation ou de la mise à niveau vers la version de VMware Tools incluse dans cette version. La mise à niveau vers la dernière version de VMware Tools n'est pas toujours nécessaire. Les nouvelles versions de VMware Tools sont compatibles avec plusieurs versions d'hôte. Pour éviter les mises à niveau inutiles, évaluez si les fonctions et les capacités ajoutées sont nécessaires pour votre environnement.

**Tableau 4-1. Options de compatibilité de la machine virtuelle**

| Compatibilité                             | Description   |
|---|---|
| ESXi 8.0 et versions ultérieures          | Cette machine virtuelle (version matérielle 20) est compatible avec ESXi 8.0 et versions ultérieures.   |
| ESXi 7.0 Update 3 et versions ultérieures | Cette machine virtuelle (version matérielle 19) est compatible avec ESXi 7.0 Update 3 et ESXi 8.0.  |
| ESXi 7.0 Update 2 et versions ultérieures | Cette machine virtuelle (version de matériel 19) est compatible avec ESXi 7.0 Update 2, ESXi 7.0 Update 3 et ESXi 8.0.  |
| ESXi 7.0 Update 1 et versions ultérieures | Cette machine virtuelle (version de matériel 18) est compatible avec ESXi 7.0 Update 1, ESXi 7.0 Update 2, ESXi 7.0 Update 3 et ESXi 8.0.   |
| ESXi 7.0 et versions ultérieures          | Cette machine virtuelle (version de matériel 17) est compatible avec ESXi 7.0, ESXi 7.0 Update 1, ESXi 7.0 Update 2, ESXi 7.0 Update 3 et ESXi 8.0.   |
| ESXi 6.7 Update 2 et versions ultérieures | Cette machine virtuelle (version de matériel 15) est compatible avec ESXi 6.7 Update 2, ESXi 6.7 Update 3, ESXi 7.0, ESXi 7.0 Update 1, ESXi 7.0 Update 2 et ESXi 7.0 Update 3 et ESXi 8.0.                     |
| ESXi 6.7 et versions ultérieures          | Cette machine virtuelle (version de matériel 14) est compatible avec ESXi 6.7, ESXi 6.7 Update 2, ESXi 6.7 Update 3, ESXi 7.0, ESXi 7.0 Update 1, ESXi 7.0 Update 2 et ESXi 7.0 Update 3 et ESXi 8.0.           |
| ESXi 6.5 et versions ultérieures          | Cette machine virtuelle (version de matériel 13) est compatible avec ESXi 6.5, ESXi 6.7, ESXi 6.7 Update 2, ESXi 6.7 Update 3, ESXi 7.0, ESXi 7.0 Update 1, ESXi 7.0 Update 2 et ESXi 7.0 Update 3 et ESXi 8.0. |

Pour plus d'informations, consultez le Guide de compatibilité de VMware à l'adresse <http://www.vmware.com/resources/compatibility>.

## Mise à niveau de VMware Tools dans VMware Host Client

Vous pouvez mettre à niveau VMware Tools sur une machine virtuelle en utilisant VMware Host Client

### Conditions préalables

Mettez la machine virtuelle sous tension.

### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Sélectionnez une machine virtuelle dans la liste.
- 3 Cliquez sur **Actions**, sélectionnez **SE invité** dans le menu déroulant, et sélectionnez **Mettre à niveau VMware Tools**.

## Configuration d'une machine virtuelle dans VMware Host Client

Vous pouvez ajouter ou configurer la plupart des propriétés de machine virtuelle pendant le procédé de création de machine virtuelle ou après que vous avez créé la machine virtuelle et installé le système d'exploitation invité.

Vous pouvez configurer trois types de propriétés de machine virtuelle.

### Matériel

Affichez la configuration matérielle existante et ajoutez ou supprimez du matériel.

### Options

Consultez et configurez un certain nombre de propriétés de machine virtuelle, telles que l'interaction de gestion de l'alimentation entre le système d'exploitation invité et la machine virtuelle, et les paramètres de VMware Tools.

### Ressources

Configurez les CPU, les sources en hyperthreading de CPU, la mémoire et les disques.

## Vérifier la version matérielle d'une machine virtuelle dans VMware Host Client

Vous pouvez vérifier la version matérielle d'une machine virtuelle en examinant la page de résumé de la machine virtuelle.

### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez sur une machine virtuelle dans la liste.

La version matérielle apparaît sous le nom de la machine virtuelle.

## Modifier le nom d'une machine virtuelle dans VMware Host Client

Vous pouvez modifier le nom d'une machine virtuelle une fois le processus de création terminé. Le fait de changer le nom ne modifie pas le nom des fichiers de machine virtuelle ni le nom du répertoire dans lequel se trouvent les fichiers.

### Conditions préalables

Mettez la machine virtuelle hors tension.

### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez avec le bouton droit sur une machine virtuelle de la liste et sélectionnez **Modifier les paramètres** dans le menu contextuel.
- 3 Cliquez sur **Options VM**.
- 4 Dans la zone de texte **Nom de la VM**, entrez le nom de la machine virtuelle.
- 5 Cliquez sur **Enregistrer**.

## Afficher l'emplacement du fichier de configuration des machines virtuelles dans VMware Host Client

Vous pouvez afficher l'emplacement des fichiers de configuration et des fichiers de travail d'une machine virtuelle en utilisant VMware Host Client.

Cette information est utile quand vous configurez des systèmes de sauvegarde.

### Conditions préalables

Mettez la machine virtuelle hors tension.

### Procédure


- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez avec le bouton droit sur la machine virtuelle et cliquez sur **Modifier les paramètres**.
- 3 Cliquez sur l'onglet **Options VM** et développez **Options générales**.
- 4 Enregistrez l'emplacement des fichiers de configuration et des fichiers de travail.
- 5 Cliquez sur **Annuler** pour quitter l'écran.

## Configurer les états d'alimentation de la machine virtuelle dans VMware Host Client

Il est utile de changer les états d'alimentation de la machine virtuelle lorsque vous assurez la maintenance de l'hôte. Vous pouvez utiliser les paramètres système par défaut pour les contrôles d'alimentation de la machine virtuelle ou configurer les contrôles pour interagir avec le système d'exploitation invité. Par exemple, vous pouvez configurer le contrôle **Mettre hors tension** pour mettre la machine virtuelle hors tension ou arrêter le système d'exploitation invité.

Vous pouvez modifier de nombreuses configurations de machine virtuelle pendant que la machine virtuelle est en cours d'exécution, mais il peut être nécessaire de changer l'état d'alimentation de la machine virtuelle pour certaines configurations.




Vous ne pouvez pas configurer une action **Mettre sous tension** (  ). Cette action met sous tension une machine virtuelle qui est arrêtée ou démarre une machine virtuelle et exécute un script si elle est suspendue et que VMware Tools est installé et disponible. Si VMware Tools n'est pas installé, elle démarre la machine virtuelle interrompue et n'exécute pas de script.

#### Conditions préalables

- Vérifiez que vous avez des privilèges pour exécuter l'opération de mise sous tension prévue sur la machine virtuelle.
- Pour définir des fonctionnalités d'alimentation facultatives, installez VMware Tools sur la machine virtuelle.
- Mettez la machine virtuelle hors tension avant de modifier les options des outils VMware Tools.

#### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez avec le bouton droit sur une machine virtuelle de la liste et sélectionnez **Modifier les paramètres** dans le menu déroulant.
- 3 Dans l'onglet **Options VM**, développez **VMware Tools**.
- 4 Sélectionnez une option pour le contrôle **Mettre hors tension** (  ) de la machine virtuelle dans le menu déroulant.

| Option                     | Description  |
|----------------------------|--|
| <b>Mettre hors tension</b> | Arrête immédiatement la machine virtuelle. Une action Mettre hors tension arrête le système d'exploitation invité ou met la machine virtuelle hors tension. Un message indique qu'il est possible que le système d'exploitation invité ne s'arrête pas correctement. Utilisez cette option de désactivation seulement si nécessaire. |
| <b>Arrêter l'invité</b>    | Utilise VMware Tools pour lancer un arrêt système en ordre de la machine virtuelle. Les opérations d'activation logicielle sont possibles seulement si les outils sont installés dans le système d'exploitation invité.  |
| <b>Système par défaut</b>  | Suit les paramètres système. La valeur actuelle des paramètres système est affichée entre parenthèses.   |

- 5 Sélectionnez une option pour le contrôle **Interrompre** () du menu déroulant.

| Option                            | Description  |
|-----------------------------------|--|
| <b>Interrompre</b>                | Fait une pause toute l'activité de machine virtuelle. Si VMware Tools est installé et disponible, une action Interrompre exécute un script et interrompt la machine virtuelle. Si VMware Tools n'est pas installé, l'action Interrompre interrompt la machine sans exécuter de script. |
| <b>Mettre l'invité en attente</b> | Fait passer le système d'exploitation invité en attente. Cette option interrompt tous les processus, mais tous les périphériques virtuels restent connectés à la machine virtuelle.  |
| <b>Système par défaut</b>         | Suit les paramètres système. La valeur actuelle des paramètres système est affichée entre parenthèses.   |

- 6 Sélectionnez une option pour le contrôle **Réinitialiser** () dans le menu déroulant.

| Option                   | Description   |
|--------------------------|---|
| <b>Réinitialiser</b>     | Arrête et redémarre le système d'exploitation invité sans mettre hors tension la machine virtuelle. Si VMware Tools n'est pas installé, l'action Réinitialiser réinitialise la machine virtuelle. |
| <b>Redémarrer Invité</b> | Utilise VMware Tools pour lancer un redémarrage ordonné. Les opérations d'activation logicielle sont possibles seulement si les outils sont installés dans le système d'exploitation invité.      |
| <b>Par défaut</b>        | Suit les paramètres système. La valeur actuelle des paramètres système est affichée entre parenthèses.  |

- 7 Cliquez sur **Enregistrer**.

## Modifier les paramètres des fichiers de configuration dans VMware Host Client

Pour résoudre certains problèmes de votre système, la documentation VMware ou un représentant de l'assistance technique VMware peut vous demander de modifier ou d'ajouter des paramètres de configuration de machine virtuelle.

**Important** La modification ou l'ajout d'un paramètre alors que votre système est stable peut entraîner une diminution des performances et une instabilité du système.

Les conditions suivantes s'appliquent :

- Pour changer un paramètre, vous devez changer la valeur existante pour la paire mot-clé/valeur. Par exemple, si la paire existante est Mot-clé/valeur, et que vous la changez en Mot-clé/valeur2, le nouveau mot-clé est valeur2.

- Vous ne pouvez pas supprimer l'entrée du paramètre de configuration.

---

**Attention** Vous devez attribuer une valeur aux mots-clés de paramètres de configuration. Si vous n'attribuez aucune valeur, il se peut que le mot-clé reçoive alors la valeur 0 ou faux, ce qui empêche de mettre sous tension la machine virtuelle.

---

#### Conditions préalables

Mettez la machine virtuelle hors tension.

#### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez avec le bouton droit sur une machine virtuelle de la liste et sélectionnez **Modifier les paramètres** dans le menu contextuel.
- 3 Dans l'onglet **Options VM**, développez **Avancé**.
- 4 Dans la ligne Paramètres de configuration, cliquez sur **Modifier la configuration**.  
La boîte de dialogue **Paramètres de Configuration** s'ouvre.
- 5 (Facultatif) Pour ajouter un paramètre, cliquez sur **Ajouter un paramètre** et entrez le nom et la valeur du paramètre.
- 6 (Facultatif) Pour changer un paramètre, tapez une nouvelle valeur dans la zone de texte **Valeur** du paramètre.
- 7 Cliquez sur **OK** pour enregistrer les modifications et quitter la boîte de dialogue **Paramètres de configuration**.
- 8 Cliquez sur **Enregistrer**.

## Configurer le démarrage automatique pour une machine virtuelle dans VMware Host Client

Configurez les options de démarrage automatique pour une machine virtuelle afin qu'elle démarre avant ou après d'autres machines virtuelles présentes sur l'hôte.

#### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez avec le bouton droit sur une machine virtuelle dans la liste.

- 3 Sélectionnez **Démarrage automatique** dans le menu contextuel et cliquez sur une option pour configurer les options de démarrage automatique pour cette machine virtuelle.

| Option                | Description  |
|-----------------------|--|
| Augmenter la priorité | Augmentez la priorité de démarrage de cette machine virtuelle pour qu'elle démarre avant d'autres machines virtuelles. |
| Réduire la priorité   | Baissez la priorité de démarrage de cette machine virtuelle pour qu'elle démarre après d'autres machines virtuelles.   |

## Mettre à niveau la compatibilité des machines virtuelles à l'aide de VMware Host Client

Le niveau de compatibilité d'une machine virtuelle détermine le matériel virtuel disponible pour la machine, ce qui correspond au matériel physique disponible sur la machine de l'hôte. Vous pouvez actualiser le niveau de compatibilité pour rendre une machine virtuelle compatible avec la version la plus récente d'ESXi qui s'exécute sur l'hôte.

Pour plus d'informations sur les versions matérielles de la machine virtuelle et la compatibilité, consultez *Administration d'une machine virtuelle vSphere*.

### Conditions préalables

- Créer une sauvegarde ou un snapshot des machines virtuelles. Reportez-vous à la section [Gérer des machines virtuelles avec des snapshots](#).
- Mise à niveau de VMware Tools. Sur les machines virtuelles qui exécutent Microsoft Windows, si vous mettez à niveau la compatibilité avant de mettre à niveau VMware Tools, la machine virtuelle peut perdre ses paramètres réseau.
- Vérifiez que tous les fichiers `.vmdk` sont disponibles sur l'hôte ESXi dans une banque de données VMFS3, VMFS5 ou NFS.
- Vérifiez que la machine virtuelle est stockée dans des banques de données VMFS3, VMFS5 ou NFS.
- Vérifiez que les paramètres de compatibilité des machines virtuelles ne sont pas définis sur la version la plus récente prise en charge.
- Déterminez les versions ESXi avec lesquelles vous souhaitez que les machines virtuelles soient compatibles. Reportez-vous à la section *Administration d'une machine virtuelle vSphere*.

### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez avec le bouton droit sur une machine virtuelle de la liste et sélectionnez **Mettre à niveau la compatibilité VM** dans le menu contextuel.
- 3 Sélectionnez la dernière version prise en charge et cliquez sur **Mise à niveau**.

## Gérer des machines virtuelles dans VMware Host Client

Après avoir créé une machine virtuelle dans VMware Host Client, vous pouvez effectuer différentes tâches de gestion sur cette machine, y compris la suppression de la machine virtuelle de l'hôte ou d'une banque de données, son ré-enregistrement sur une banque de données, etc. Vous pouvez également renvoyer la machine virtuelle vers l'hôte.

### Accès à une machine virtuelle dans VMware Host Client

Vous pouvez accéder aux machines virtuelles présentes sur l'hôte auquel vous êtes connecté, pour configurer le matériel et les options des machines virtuelles, pour effectuer des tâches administratives et pour effectuer des tâches de dépannage de base.

Pour afficher une machine virtuelle dans l'inventaire VMware Host Client, mettez la machine virtuelle sous tension.

#### Procédure

- ◆ Pour accéder aux machines virtuelles qui sont disponibles sur l'hôte auquel vous êtes connecté, cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.

#### Résultats

La liste des machines virtuelles disponibles est affichée sous **Machines virtuelles**.

Vous pouvez désormais modifier les paramètres des machines virtuelles et effectuer différentes tâches administratives et de dépannage sur les machines virtuelles de la liste.

## États d'alimentation d'une machine virtuelle dans VMware Host Client

Les opérations d'alimentation de base d'une machine virtuelle incluent la mise sous tension, la mise hors tension, l'interruption et la réinitialisation.

Pour plus d'informations sur la modification des états d'alimentation d'une machine virtuelle, reportez-vous à la section [Configurer les états d'alimentation de la machine virtuelle dans VMware Host Client](#).





#### Conditions préalables

- Vérifiez que vous disposez du privilège **Machine virtuelle.Interaction.Mettre sous tension**.
- Vérifiez que vous disposez du privilège **Machine virtuelle.Interaction.Mettre hors tension**.
- Vérifiez que vous disposez du privilège **Machine virtuelle.Interaction.Interrompre**.
- Vérifiez que vous disposez du privilège **Machine virtuelle.Interaction.Réinitialiser**.

#### Procédure

- 1 Dans l'inventaire de VMware Host Client, cliquez sur **Machines virtuelles**.

- 2 Cliquez avec le bouton droit sur une machine virtuelle et sélectionnez une opération d'alimentation.

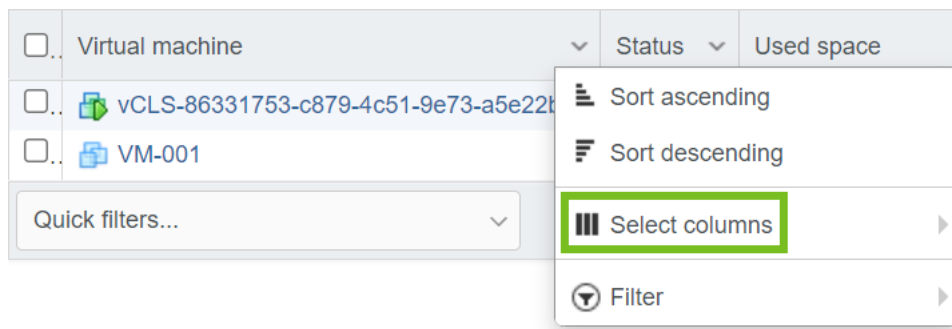
| Option  | Description   |
|---|---|
| Mettre sous tension (  ) | Met sous tension une machine virtuelle lorsque la machine virtuelle est arrêtée.  |
| Mettre hors tension (  ) | Met hors tension une machine virtuelle et arrête le système d'exploitation invité. La mise hors tension d'une machine virtuelle peut entraîner une perte de données.  |
| Interrompre (  )         | Interrompt une machine virtuelle en cours d'exécution et la laisse connectée au réseau. Lorsque vous relancez une machine virtuelle interrompue, celle-ci continue à fonctionner au même point où elle se trouvait au moment de son interruption. |
| Réinitialiser (  )       | Arrête et redémarre le système d'exploitation invité sans mettre hors tension la machine virtuelle.   |

## Utiliser la configuration des colonnes des machines virtuelles dans VMware Host Client

Le panneau des machines virtuelles dans VMware Host Client vous permet de configurer les informations que vous souhaitez afficher. Vous pouvez afficher ou masquer différentes colonnes, telles que l'état, l'espace utilisé, le nom d'hôte, le CPU de l'hôte, etc.

### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Dans la liste des machines virtuelles, cliquez sur l'icône de flèche vers le bas en regard de n'importe quel titre de colonne et sélectionnez **Sélectionner des**



colonnes.

La liste contenant toutes les colonnes disponibles s'affiche.

- 3 Sélectionnez les informations que vous souhaitez afficher dans le panneau de la machine virtuelle.

## Supprimer des machines virtuelles d'un hôte dans VMware Host Client

Vous pouvez désinscrire une machine virtuelle si vous souhaitez la conserver dans la banque de données mais que vous ne souhaitez plus la voir affichée dans l'inventaire VMware Host Client.

### Conditions préalables

Mettez la machine virtuelle hors tension.

### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez avec le bouton droit de la souris sur une machine virtuelle de la liste et sélectionnez **Désinscrire**.
- 3 Pour confirmer que vous voulez supprimer la machine virtuelle de l'inventaire, cliquez sur **Oui**.

### Résultats

L'hôte supprime la machine virtuelle de l'inventaire et n'assure plus le suivi de sa condition.

## Supprimer des machines virtuelles de la banque de données dans VMware Host Client

Pour libérer de l'espace sur la banque de données, vous pouvez supprimer les machines virtuelles dont vous n'avez plus besoin. La suppression d'une machine virtuelle de l'inventaire VMware Host Client supprime tous les fichiers de la machine virtuelle de la banque de données, y compris le fichier de configuration et les fichiers de disques virtuels. Vous pouvez supprimer plusieurs machines virtuelles.

### Conditions préalables

- Mettez la machine virtuelle hors tension.
- Vérifiez que la machine virtuelle ne partage pas le disque avec une autre machine virtuelle. Si deux machines virtuelles partagent un disque, les fichiers de disque ne sont pas supprimés.

### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cochez une ou plusieurs cases en regard des machines virtuelles que vous souhaitez supprimer et sélectionnez **Actions > Supprimer**.

La boîte de dialogue **Supprimer des machines virtuelles** s'ouvre.

- 3 Cliquez sur **Supprimer**.

## Enregistrer une machine virtuelle dans VMware Host Client

Si vous supprimez une machine virtuelle ou un modèle d'un hôte sans les supprimer de la banque de données de cet hôte, vous pouvez les renvoyer vers l'inventaire de l'hôte.

## Procédure

- 1 Cliquez sur **Stockage** dans l'inventaire VMware Host Client.
- 2 Cliquez avec le bouton droit sur une banque de données dans la liste, puis cliquez sur **Enregistrer une machine virtuelle**.
- 3 Sélectionnez la machine virtuelle à enregistrer dans la liste et cliquez sur **Enregistrer**.

## Gérer des machines virtuelles avec des snapshots

Un snapshot conserve l'état et les données d'une machine virtuelle au moment de sa création. Lorsque vous prenez un snapshot d'une machine virtuelle, une image de la machine virtuelle à un état donné est copiée et stockée. Les snapshots sont utiles quand vous souhaitez rétablir à plusieurs reprises un état de machine virtuelle donné, mais que vous ne voulez pas créer plusieurs machines virtuelles.

Vous pouvez créer plusieurs snapshots d'une machine virtuelle pour créer des positions de restauration au cours d'un processus linéaire. Avec plusieurs snapshots, vous pouvez sauvegarder plusieurs positions pour vous adapter à plusieurs types de processus de travail. Les snapshots concernent les machines virtuelles individuelles. Pour créer des snapshots de plusieurs machines virtuelles, par exemple, prendre un snapshot de machine virtuelle pour chaque membre d'une équipe, vous devez créer un snapshot distinct de la machine virtuelle de chaque membre de l'équipe.

Les snapshots sont utiles en tant que solution à court terme pour tester un logiciel dont les effets sont inconnus ou potentiellement dangereux. Vous pouvez utiliser un snapshot comme point de restauration pendant un processus linéaire ou itératif, tel que l'installation de packages de mise à niveau, ou pendant un processus d'embranchement, tel que l'installation de différentes versions d'un programme. L'utilisation de snapshots garantit que chaque installation commence par une ligne de base identique.

Avec les snapshots, vous pouvez conserver une ligne de base avant de modifier une machine virtuelle.

Plusieurs options de création et de gestion des snapshots de machines virtuelles et des arborescences de snapshots sont disponibles dans vSphere Client. Ces opérations vous permettent de créer des snapshots, de restaurer un snapshot dans la hiérarchie des snapshots, de supprimer des snapshots, et bien plus encore. Vous pouvez créer des arborescences de snapshots dans lesquelles vous enregistrez l'état de la machine virtuelle à un moment donné afin de pouvoir restaurer cet état de machine virtuelle ultérieurement. Chaque branche d'une arborescence de snapshot peut contenir jusqu'à 32 snapshots.

Un snapshot conserve les informations suivantes :

- Paramètres de la machine virtuelle. Répertoire de machine virtuelle contenant les disques qui ont été ajoutés ou modifiés après la création du snapshot.
- État de l'alimentation. La machine virtuelle peut être sous tension, hors tension ou interrompue.



- État du disque. État de tous les disques virtuels de la machine virtuelle.
- État de la mémoire (facultatif). Contenu de la mémoire de la machine virtuelle.

## Hiérarchie des snapshots

vSphere Client présente la hiérarchie des snapshots sous la forme d'une arborescence dotée d'une ou de plusieurs branches. Les snapshots de la hiérarchie ont des relations parent-enfant. Dans les processus linéaires, chaque snapshot a un parent et un enfant, excepté le dernier snapshot qui n'a aucun enfant. Chaque snapshot parent peut avoir plusieurs enfants. Vous pouvez restaurer le snapshot parent ou restaurer tout snapshot parent ou enfant dans l'arborescence de snapshot et créer plusieurs snapshots à partir de ce snapshot. Chaque fois que vous restaurez un snapshot et prenez un autre snapshot, une branche (un snapshot enfant) est créée.

### Snapshots parents

Le premier snapshot de la machine virtuelle que vous créez est le snapshot parent de base. Le snapshot parent est la version récemment sauvegardée de l'état actuel de la machine virtuelle. La création d'un snapshot génère un fichier de disque delta pour chaque disque relié à la machine virtuelle et, en option, un fichier de mémoire. Les fichiers de disque delta et le fichier de mémoire sont stockés avec le fichier `.vmdk` de base. Le snapshot parent est toujours le snapshot qui s'affiche immédiatement au-dessus de l'icône **Vous êtes ici** dans le Gestionnaire de snapshots. Si vous restaurez un snapshot, ce snapshot devient le parent de l'état actuel **Vous êtes ici**.

---

**Note** Le snapshot parent n'est pas toujours le snapshot que vous avez pris le plus récemment.

---

### Snapshots enfants

Un snapshot d'une machine virtuelle créé après le snapshot parent. Chaque snapshot enfant contient les fichiers delta de chaque disque virtuel relié et, éventuellement, un fichier de mémoire qui indique l'état actuel du disque virtuel (Vous êtes ici). Les fichiers delta de chaque snapshot enfant fusionnent avec le snapshot de chaque snapshot enfant précédent jusqu'à atteindre les disques parents. Un disque enfant peut ensuite devenir le disque parent de futurs disques enfants.

La relation des snapshots parents et enfants peut évoluer si l'arborescence de snapshot possède plusieurs branches. Un snapshot parent peut avoir plusieurs enfants. Beaucoup de snapshots n'ont aucun enfant.

---

**Attention** Ne manipulez pas manuellement les disques enfants individuels ou tout fichier de configuration de snapshot car vous pourriez compromettre l'arborescence et provoquer une perte de données. Cette restriction inclut le redimensionnement des disques et les modifications apportées au disque parent de base en utilisant la commande `vmkfstools`.

---

## Comportement des snapshots

La création d'un snapshot préserve l'état du disque à un moment précis en créant une série de disques delta pour chaque disque virtuel relié ou RDM virtuel, et peut également préserver l'état de la mémoire et de l'alimentation en créant un fichier de mémoire. La création d'un snapshot génère un objet de snapshots dans le Gestionnaire de snapshot qui représente l'état et les paramètres de la machine virtuelle.

Chaque snapshot crée un autre fichier de disque delta `.vmdk`. Lorsque vous créez un snapshot, le mécanisme du snapshot empêche le système d'exploitation invité d'écrire sur le fichier `.vmdk` de base et dirige toutes les écritures vers le fichier de disque delta. Le disque delta représente la différence entre l'état actuel du disque virtuel et son état lors de la création du snapshot précédent. Si plusieurs snapshots existent, les disques delta peuvent représenter la différence entre chaque snapshot. Les fichiers de disque delta peuvent s'étendre rapidement et devenir aussi importants que le disque virtuel si le système d'exploitation invité écrit sur chaque bloc du disque virtuel.

## Fichiers de snapshot

Lorsque vous créez un snapshot, vous capturez l'état des paramètres de la machine virtuelle du disque virtuel. Si vous créez un snapshot de mémoire, vous capturez également l'état de la mémoire de la machine virtuelle. Ces états sont sauvegardés dans des fichiers situés au même emplacement que les fichiers de base de la machine virtuelle.

### Fichiers de snapshot

Une machine virtuelle se compose de fichiers stockés sur un périphérique de stockage compatible. Une opération Prendre un snapshot crée des fichiers `.vmdk`, `-delta.vmdk`, `.vmsd` et `.vmsn`. Par défaut, le premier disque et tous les disques delta sont stockés avec le fichier `.vmdk`. Les fichiers `.vmsd` et `.vmsn` sont stockés dans le répertoire de la machine virtuelle.

### Fichiers de disque delta

Fichier `.vmdk` sur lequel le système d'exploitation peut écrire. Le disque delta représente la différence entre l'état actuel du disque virtuel et son état lors de la création du snapshot précédent. Lorsque vous créez un snapshot, l'état du disque virtuel est préservé, le système d'exploitation invité cesse d'écrire sur le disque, et un disque delta ou enfant est créé.

Un disque delta a deux fichiers. Le premier est un petit fichier descripteur qui contient des informations sur le disque virtuel, telles que des informations de relation parent-enfant et de géométrie. L'autre est un fichier correspondant qui contient les données brutes.

Les fichiers qui constituent le disque delta sont appelés disques enfants ou fichiers redo-log.

### Fichier plat

Fichier `-flat.vmdk` correspondant à l'un des deux fichiers constituant le disque de base. Le disque plat contient les données brutes du disque de base. Ce fichier n'apparaît pas en tant que fichier séparé dans le navigateur de banque de données.

## Fichier de base de données

Fichier `.vmsd` contenant des informations sur les snapshots de la machine virtuelle et principale source d'information du Gestionnaire de snapshot. Ce fichier contient des entrées de ligne qui définissent les relations entre les snapshots et entre les disques enfants de chaque snapshot.

## Fichier de mémoire

Fichier `.vmsn` contenant l'état actif de la machine virtuelle. En capturant l'état de la mémoire de la machine virtuelle, vous pouvez rétablir la machine virtuelle à un état sous tension. Avec les snapshots qui ne sont pas des snapshots de mémoire, vous pouvez uniquement rétablir la machine virtuelle à un état hors tension. Les snapshots de mémoire sont plus longs à créer que les autres snapshots. Le temps requis par l'hôte ESXi pour écrire la mémoire sur le disque dépend de la quantité de mémoire configurée sur la machine virtuelle.

Une opération **Prendre un snapshot** crée des fichiers `.vmdk`, `-delta.vmdk`, `vmsd` et `vmsn`.

| Fichier  | Description   |
|--|---|
| <code>vmname-number.vmdk</code> et <code>vmname-number-delta.vmdk</code> | <p>Le fichier de snapshot représente la différence entre l'état actuel du disque virtuel et son état lors de la création du snapshot précédent.</p> <p>Le nom de fichier utilise la syntaxe suivante, <code>S1vm-000001.vmdk</code>, où <code>S1vm</code> est le nom de la machine virtuelle et le nombre à six chiffres, <code>000001</code>, est basé sur les fichiers qui existent déjà dans le répertoire. Le nombre ne tient pas compte du nombre de disques attachés à la machine virtuelle.</p>                          |
| <code>vmname.vmsd</code>   | Base de données contenant des informations sur les snapshots de la machine virtuelle et principale source d'information du Gestionnaire de snapshot.  |
| <code>vmname.Snapshotnumber.vmsn</code>                                  | <p>État de la mémoire de la machine virtuelle au moment de la création du snapshot. Le nom de fichier utilise la syntaxe suivante, <code>S1vm.snapshot1.vmsn</code>, où <code>S1vm</code> est le nom de la machine virtuelle et <code>snapshot1</code> le premier snapshot.</p> <p><b>Note</b> Un fichier <code>.vmsn</code> est créé chaque fois que vous créez un snapshot, quelle que soit la sélection de mémoire. Un fichier <code>.vmsn</code> sans mémoire est beaucoup plus petit qu'un fichier doté d'une mémoire.</p> |

## Limitations des snapshots

Les snapshots peuvent affecter les performances des machines virtuelles et ne prennent pas en charge certains types de disques ou des machines virtuelles configurés avec le partage de bus. Les snapshots sont utiles en tant que solutions à court terme pour capturer des états de machine virtuelle instantanés et ne sont pas adaptés aux sauvegardes de machine virtuelle à long terme.

- VMware ne prend pas en charge les snapshots des disques bruts, des disques en mode physique RDM ou des systèmes d'exploitation invités qui utilisent un initiateur iSCSI sur le client.
- Les machines virtuelles disposant de disques indépendants doivent être mises hors tension avant de créer un snapshot. Les machines virtuelles sous tension dotées de disques indépendants ne peuvent pas prendre en charge les snapshots de mémoire.

- Les snapshots mis au repos requièrent l'installation de VMware Tools et la prise en charge des systèmes d'exploitation invités.
- Les snapshots ne sont pas pris en charge avec les périphériques PCI vSphere DirectPath I/O.
- VMware ne prend pas en charge les snapshots des machines virtuelles configurées avec le partage de bus. Si vous voulez utiliser le partage de bus, envisagez d'exécuter le logiciel de sauvegarde dans le système d'exploitation client comme une solution alternative. Si la machine virtuelle dispose actuellement de snapshots et qu'elle ne permet pas de configurer le partage de bus, supprimez (consolidez) les snapshots.
- Les snapshots fournissent une image instantanée du disque que les solutions de sauvegarde peuvent utiliser, mais les snapshots ne sont pas conçus comme une méthode de sauvegarde ou de récupération robuste. Si les fichiers contenant une machine virtuelle sont perdus, ses fichiers de snapshot sont également perdus. En outre, un grand nombre de snapshots sont difficiles à gérer, prennent beaucoup d'espace sur le disque et ne sont pas protégés en cas de panne du matériel.
- Les snapshots peuvent affecter d'une manière négative les performances d'une machine virtuelle. La dégradation des performances est basée sur la durée pendant laquelle le snapshot ou l'arborescence de snapshot reste en place, la profondeur de l'arborescence et l'étendue des modifications de la machine virtuelle et de son système d'exploitation invité depuis la création du snapshot. En outre, vous pourriez observer un retard lors de la mise sous tension de la machine virtuelle. N'exécutez pas des machines virtuelles de production à partir de snapshots de façon permanente.
- Si une machine virtuelle dispose de disques durs d'une capacité supérieure à 2 To, l'exécution des opérations de snapshot peut être beaucoup plus longue.

## Créer un snapshot d'une machine virtuelle dans VMware Host Client

Vous pouvez créer un ou plusieurs snapshots d'une machine virtuelle pour capturer l'état des paramètres, du disque et de la mémoire au moment où vous créez ce snapshot. Lorsque vous créez un snapshot, vous pouvez également mettre au repos les fichiers de machine virtuelle et exclure les disques de machine virtuelle des snapshots. Vous pouvez créer un snapshot lorsqu'une machine virtuelle est sous tension, hors tension ou suspendue. Pour créer un snapshot d'une machine virtuelle interrompue, attendez la fin de l'opération d'interruption.

Lorsque vous prenez un snapshot, l'autre activité qui se déroule sur la machine virtuelle pourrait affecter le processus de snapshot lors du retour à ce snapshot. Du point de vue du stockage, il est préférable de prendre un snapshot lorsque vous n'appliquez pas une charge E/S importante. Du point de vue du fonctionnement, il est préférable de prendre un snapshot lorsqu'aucune application de la machine virtuelle ne communique avec d'autres ordinateurs. La probabilité qu'un problème survienne est plus grande si la machine virtuelle communique avec un autre ordinateur, surtout dans un environnement de production. Par exemple, si vous prenez un snapshot tandis que la machine virtuelle télécharge un fichier d'un serveur sur le réseau, la machine virtuelle

continue de télécharger le fichier, communiquant sa progression au serveur. Si vous retournez au snapshot, les communications entre la machine virtuelle et le serveur sont confuses et le transfert de fichier échoue. Selon la tâche que vous êtes en train de réaliser, vous pouvez créer un snapshot de mémoire ou bien mettre au repos le système de fichiers de la machine virtuelle.

### Snapshots de mémoire

Sélection par défaut pour la création de snapshots. Lorsque vous capturez l'état de la mémoire de la machine virtuelle, le snapshot conserve l'état actif de la machine virtuelle. Les snapshots de mémoire permettent de créer un snapshot à un instant précis (par exemple, pour mettre à niveau un logiciel qui fonctionne parfaitement). Si vous créez un snapshot de mémoire et que la mise à niveau ne s'exécute pas correctement, ou si le logiciel ne vous convient pas, vous pouvez restaurer l'état précédent de la machine virtuelle.

Lorsque vous capturez l'état de la mémoire, les fichiers de la machine virtuelle ne nécessitent aucune mise au repos. Si vous ne capturez pas l'état de la mémoire, le snapshot ne sauvegarde pas l'état actif de la machine virtuelle et les disques sont résilients à moins que vous ne les mettiez au repos.

L'exécution des snapshots qui capturent l'état de la mémoire d'une machine virtuelle est plus longue. Il est possible que vous observiez une pause momentanée de la réponse sur le réseau.

### Snapshots mis au repos

Lorsque vous mettez au repos une machine virtuelle, VMware Tools met au repos le système de fichiers de la machine virtuelle. Une opération de mise au repos garantit qu'un disque de snapshot représente un état cohérent des systèmes de fichiers invités. L'opération de mise au repos met en pause ou altère l'état des processus en cours d'exécution sur la machine virtuelle, en particulier les processus susceptibles de modifier les informations stockées sur le disque lors d'une opération de restauration. Les snapshots mis au repos s'utilisent notamment lors des sauvegardes automatisées ou périodiques. Par exemple, si vous méconnaissiez l'activité de la machine virtuelle, mais que vous souhaitez disposer de plusieurs sauvegardes récentes, vous pouvez mettre les fichiers au repos.

Si la machine virtuelle est hors tension ou si VMware Tools n'est pas disponible, le paramètre *Quiesce* n'est pas disponible. Les machines virtuelles équipées de disques haute capacité ne peuvent pas être mises au repos.

La suspension avec cohérence des applications n'est pas prise en charge pour les machines virtuelles possédant des disques IDE ou SATA.

---

**Important** Les snapshots ne doivent pas être utilisés comme unique solution de sauvegarde, ni comme solution de sauvegarde sur le long terme.

---

**Note** Si vous créez un snapshot d'un disque dynamique (type de disque spécifique à Microsoft), la technologie des snapshots préserve l'état de mise au repos du système de fichiers, mais pas l'état de mise au repos de l'application.

---

## Conditions préalables

- Si vous créez un snapshot de la mémoire d'une machine virtuelle possédant plusieurs disques dans différents modes de disque, vérifiez que la machine virtuelle est hors tension. Par exemple, si vous avez une configuration à but précis qui exige que vous utilisiez un disque indépendant, vous devez mettre hors tension la machine virtuelle avant de prendre un snapshot.
- Pour capturer l'état de la mémoire de la machine virtuelle, vérifiez que la machine virtuelle est sous tension.
- Pour suspendre les fichiers de la machine virtuelle, vérifiez que la machine virtuelle est sous tension et que VMware Tools est installé.
- Vérifiez que vous disposez du privilège **Machine virtuelle.Gestion des snapshots.Créer un snapshot** sur la machine virtuelle.

## Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez avec le bouton droit sur la machine virtuelle dans la liste et sélectionnez **Snapshots > Créer un snapshot**.
- 3 Entrez un nom pour le snapshot.
- 4 (Facultatif) Tapez la description du snapshot.
- 5 (Facultatif) Cochez la case **Prendre un snapshot de la mémoire de la machine virtuelle** pour capturer la mémoire de la machine virtuelle.
- 6 (Facultatif) Décochez la case **Prendre un snapshot de la mémoire de la machine virtuelle** et cochez la case **Mettre au repos le système de fichiers client (VMware Tools installé)** pour suspendre les processus en cours dans le système d'exploitation invité afin que le contenu du système de fichiers ait un état cohérent connu lors de la création du snapshot.

Suspendez les fichiers de la machine virtuelle uniquement lorsque celle-ci est sous tension et que vous ne voulez pas capturer la mémoire de la machine virtuelle.

- 7 Cliquez sur **Créer un snapshot**.

## Restaurer le snapshot le plus récent dans VMware Host Client

Pour restaurer une machine virtuelle à son état d'origine ou pour rétablir un autre snapshot dans la hiérarchie des snapshots, vous pouvez restaurer un snapshot.

Lorsque vous rétablissez un snapshot, vous restaurez la mémoire, les paramètres et l'état de la machine virtuelle, ainsi que l'état de ses disques, qui existaient au moment de la création du snapshot. Si vous souhaitez que la machine virtuelle soit interrompue, mise sous tension ou mise hors tension lorsque vous la démarrez, assurez-vous qu'elle est en bon état lorsque vous créez le snapshot.

Vous pouvez rétablir les snapshots comme suit :

### Restaurer le dernier snapshot

Restaure le snapshot parent à un niveau supérieur de la hiérarchie par rapport à la position **Vous êtes ici**. **Restaurer vers le dernier snapshot** active le snapshot parent de l'état actuel de la machine virtuelle.

### Restaurer

Vous permet de rétablir tout snapshot de l'arborescence et de faire de ce snapshot le snapshot parent de l'état actuel de la machine virtuelle. Les snapshots enfants ultérieurs à ce point créent une nouvelle branche dans l'arborescence.

La restauration des snapshots a les effets suivants :

- Les états actuels du disque et de la mémoire sont ignorés et la machine virtuelle revient aux états du disque et de la mémoire du snapshot parent.
- Les snapshots existants sont supprimés. Vous pouvez restaurer ces snapshots à tout moment.
- Si le snapshot inclut l'état de la mémoire, la machine virtuelle sera dans le même état d'alimentation que lorsque vous avez créé le snapshot.

**Tableau 4-2. État d'alimentation de la machine virtuelle après la restauration d'un snapshot**

| État de la machine virtuelle lors de la création d'un snapshot parent | État de la machine virtuelle après la restauration                                       |
|---|--|
| Sous tension (inclut la mémoire)                                      | Revient au snapshot parent, puis la machine virtuelle est mise sous tension et exécutée. |
| Sous tension (n'inclut pas la mémoire)                                | Revient au snapshot parent, puis la machine virtuelle est mise hors tension.             |
| Hors tension (n'inclut pas la mémoire)                                | Revient au snapshot parent, puis la machine virtuelle est mise hors tension.             |

Les machines virtuelles exécutant certains types de charges de travail peuvent demander plusieurs minutes pour redevenir réactives après un retour à partir d'un snapshot.

**Note** Les métadonnées vApp des machines virtuelles des vApp ne suivent pas la sémantique de snapshots pour la configuration de machine virtuelle. Les propriétés de vApp qui sont supprimées, modifiées ou définies après la création d'un snapshot restent intactes (supprimées, modifiées ou définies) après que la machine virtuelle retourne à ce snapshot ou à tout snapshot antérieur.

### Conditions préalables

Vérifiez que vous disposez du privilège **Machine virtuelle.Gestion des snapshots.Restaurer un snapshot** sur la machine virtuelle.

### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.

- 2 Cliquez avec le bouton droit sur la machine virtuelle dans la liste et sélectionnez **Snapshots > Restaurer le snapshot**.

---

**Note** L'état actuel de la machine virtuelle sera détruit sauf s'il a été sauvegardé dans un snapshot.

---

- 3 Cliquez sur **Restaurer** pour restaurer la machine virtuelle sur le snapshot le plus récent.

## Supprimer un snapshot dans VMware Host Client

Vous pouvez utiliser le Gestionnaire de snapshots pour supprimer l'un des snapshots ou tous les snapshots d'une arborescence. Lorsque vous effacez un snapshot, il est supprimé du Gestionnaire de snapshot. Les fichiers de snapshot sont consolidés et écrits sur le disque de snapshot parent et fusionnent avec le disque de base de la machine virtuelle.

La suppression d'un snapshot ne modifie pas la machine virtuelle ni les autres snapshots. La suppression d'un snapshot consolide les modifications entre les snapshots et les précédents états de disque et écrit toutes les données du disque delta qui contient les informations sur le snapshot supprimé sur le disque parent. Lorsque vous supprimez le snapshot parent de base, toutes les modifications fusionnent avec le disque de base de la machine virtuelle.

Pour supprimer un snapshot, un volume important d'informations doit être lu et écrit sur un disque. Ce processus peut réduire les performances des machine virtuelles jusqu'à ce que la consolidation soit effectuée. La consolidation des snapshots supprime les disques redondants, ce qui améliore les performances de la machine virtuelle et économise de l'espace de stockage. Le temps nécessaire pour supprimer les snapshots et consolider les fichiers de snapshot varie en fonction de la quantité de données que le système d'exploitation invité écrit sur les disques virtuels une fois que vous avez créé le dernier snapshot. Le temps nécessaire est proportionnel à la quantité de données que la machine virtuelle écrit pendant la consolidation si celle-ci est sous tension.

L'échec de la consolidation du disque peut diminuer la performance des machines virtuelles. Vous pouvez vérifier si des machines virtuelles nécessitent des opérations de consolidation distinctes en affichant une liste. Pour obtenir des informations sur l'emplacement et l'affichage de l'état de consolidation de plusieurs machines virtuelles et l'exécution d'une opération de consolidation séparée, reportez-vous à *Administration d'une machine virtuelle vSphere*

### Supprimer

Utilisez l'option **Supprimer** pour supprimer un snapshot parent ou enfant de l'arborescence de snapshot. **Supprimer** écrit les modifications du disque qui ont lieu entre l'état du snapshot et l'état du disque précédent sur le snapshot parent.

---

**Note** La suppression d'un seul snapshot préserve l'état actuel de la machine virtuelle et n'affecte aucun autre snapshot.

---



Vous pouvez également utiliser l'option **Supprimer** pour supprimer un snapshot corrompu et ses fichiers d'une branche abandonnée de l'arborescence de snapshot sans les fusionner avec le snapshot parent.

### Supprimer tout

Utilisez l'option **Supprimer tout** pour supprimer tous les snapshots du Gestionnaire de snapshot. L'option **Supprimer tout** consolide et écrit les modifications apportées entre les snapshots et les précédents états de disque delta sur le disque parent de base et les fusionne au disque de base de la machine virtuelle.

Pour empêcher les fichiers de snapshot de fusionner avec le snapshot parent, par exemple, en cas d'échec des mises à jour ou des installations, utilisez d'abord la commande **Restaurer** pour restaurer le précédent snapshot. Cette action annule les disques delta de snapshot et supprime le fichier de mémoire. Vous pouvez ensuite utiliser l'option **Supprimer** pour supprimer le snapshot et tous les fichiers associés.

Prenez garde de ne pas supprimer par accident un snapshot dont vous avez besoin. Vous ne pourrez pas restaurer un snapshot qui a été supprimé. Par exemple, vous pouvez installer plusieurs navigateurs, a, b et c, et capturer l'état de la machine virtuelle après avoir installé chaque navigateur. Le premier snapshot, ou snapshot de base, capture la machine virtuelle avec le navigateur a et le deuxième snapshot capture le navigateur b. Si vous restaurez le snapshot de base qui contient le navigateur a et que vous utilisez un troisième snapshot pour capturer le navigateur c et que vous supprimez le snapshot qui contient le navigateur b, vous ne pourrez pas revenir à l'état où la machine virtuelle contient le navigateur b.

### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez avec le bouton droit sur la machine virtuelle dans la liste et sélectionnez **Snapshots > Gérer les snapshots**.
- 3 Cliquez sur le snapshot que vous voulez supprimer, puis cliquez sur **Supprimer le snapshot**.
- 4 (Facultatif) Dans la boîte de dialogue **Supprimer le snapshot**, cochez la case **Supprimer tous les snapshots enfants** pour supprimer le snapshot sélectionné en même temps que tous ses snapshots enfants.
- 5 Cliquez sur **Supprimer** pour confirmer la suppression.
- 6 Cliquez sur **Fermer** pour sortir du Gestionnaire de snapshots.

## Suppression des snapshots

Lorsque vous effacez un snapshot, il est supprimé du Gestionnaire de snapshot. Les fichiers de snapshot sont consolidés et écrits sur le disque de snapshot parent et fusionnent avec le disque de base de la machine virtuelle.

La suppression d'un snapshot ne modifie pas la machine virtuelle ni les autres snapshots. La suppression d'un snapshot consolide les modifications entre les snapshots et les précédents états de disque et écrit toutes les données du disque delta qui contient les informations sur le snapshot supprimé sur le disque parent. Lorsque vous supprimez le snapshot parent de base, toutes les modifications fusionnent avec le disque de base de la machine virtuelle.

Pour supprimer un snapshot, un volume important d'informations doit être lu et écrit sur un disque. Ce processus peut réduire les performances des machines virtuelles jusqu'à ce que la consolidation soit effectuée. La consolidation des snapshots supprime les disques redondants, ce qui améliore les performances de la machine virtuelle et économise de l'espace de stockage. Le temps nécessaire pour supprimer les snapshots et consolider les fichiers de snapshot varie en fonction de la quantité de données que le système d'exploitation invité écrit sur les disques virtuels une fois que vous avez créé le dernier snapshot. Le temps nécessaire est proportionnel à la quantité de données que la machine virtuelle écrit pendant la consolidation si celle-ci est sous tension.

L'échec de la consolidation du disque peut diminuer la performance des machines virtuelles. Vous pouvez vérifier si des machines virtuelles nécessitent des opérations de consolidation distinctes en affichant une liste. Pour obtenir des informations sur l'emplacement et l'affichage de l'état de consolidation de plusieurs machines virtuelles et l'exécution d'une opération de consolidation séparée, reportez-vous à *Administration d'une machine virtuelle vSphere*

## Supprimer

Utilisez l'option **Supprimer** pour supprimer un snapshot parent ou enfant de l'arborescence de snapshot. **Supprimer** écrit les modifications du disque qui ont lieu entre l'état du snapshot et l'état du disque précédent sur le snapshot parent.

---

**Note** La suppression d'un seul snapshot préserve l'état actuel de la machine virtuelle et n'affecte aucun autre snapshot.

---

Vous pouvez également utiliser l'option **Supprimer** pour supprimer un snapshot corrompu et ses fichiers d'une branche abandonnée de l'arborescence de snapshot sans les fusionner avec le snapshot parent.

## Supprimer tout

Utilisez l'option **Supprimer tout** pour supprimer tous les snapshots du Gestionnaire de snapshot. L'option **Supprimer tout** consolide et écrit les modifications apportées entre les snapshots et les précédents états de disque delta sur le disque parent de base et les fusionne au disque de base de la machine virtuelle.

Pour empêcher les fichiers de snapshot de fusionner avec le snapshot parent, par exemple, en cas d'échec des mises à jour ou des installations, utilisez d'abord la commande **Restaurer** pour restaurer le précédent snapshot. Cette action annule les disques delta de snapshot et supprime le fichier de mémoire. Vous pouvez ensuite utiliser l'option **Supprimer** pour supprimer le snapshot et tous les fichiers associés.

## Pourquoi utiliser le gestionnaire de snapshots dans VMware Host Client

Vous pouvez consulter tous les snapshots de vos machines virtuelles et utiliser le Gestionnaire de snapshots pour gérer les snapshots.

Après avoir créé un snapshot, vous pouvez cliquer avec le bouton droit sur une machine virtuelle et cliquer sur **Restaurer le snapshot** pour restaurer la machine virtuelle à l'état du snapshot à n'importe quel moment.

Si vous possédez une série de snapshots, vous pouvez utiliser le Gestionnaire de snapshots pour restaurer un snapshot parent ou enfant. Les snapshots enfants ultérieurs que vous créez à partir du snapshot restauré créent une branche dans l'arborescence de snapshot. Utilisez le Gestionnaire des snapshots pour supprimer un snapshot de l'arborescence.

Tableau 4-3. Gestionnaire de snapshot

| Option                                       | Description   |
|--|---|
| Arborescence de snapshot                     | Affiche tous les snapshots de la machine virtuelle.   |
| Icône <b>Vous êtes ici</b>                   | L'icône <b>Vous êtes ici</b> représente l'état actuel et actif de la machine virtuelle.<br>Les actions <b>Restaurer</b> , <b>Supprimer</b> et <b>Modifier</b> sont désactivées pour l'état <b>Vous êtes ici</b> .   |
| <b>Créer, Restaurer, Supprimer, Modifier</b> | Options de snapshot.  |
| Détails                                      | Affiche le nom et la description du snapshot, sa date de création. La console affiche l'état de l'alimentation de la machine virtuelle lorsqu'un snapshot a été pris. Les zones de texte Nom, Description et Créé sont vides si vous ne sélectionnez pas de snapshot. |

## Surveiller une machine virtuelle dans VMware Host Client

Vous pouvez surveiller les différents aspects de performances et effectuer le suivi des actions qui ont lieu sur des machines virtuelles que vous créez dans VMware Host Client.

### Afficher les graphiques de performances des machines virtuelles dans VMware Host Client

Vous pouvez afficher des graphiques linéaires offrant des informations sur l'utilisation des ressources des machines virtuelles que vous créez dans VMware Host Client.

#### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez sur une machine virtuelle dans la liste.
- 3 Développez la machine virtuelle dans l'inventaire VMware Host Client et cliquez sur **Surveiller**.
- 4 Cliquez sur **Performance**.

- 5 Pour afficher l'utilisation des ressources des machines virtuelles au cours de la dernière heure, sélectionnez une option dans le menu déroulant.
  - Pour afficher le pourcentage de CPU que la machine virtuelle a utilisé au cours de la dernière heure, sélectionnez **Utilisation du CPU**.
  - Pour afficher la mémoire que l'hôte a consommée pendant la dernière heure, sélectionnez **Utilisation de la mémoire**.

## Afficher les événements des machines virtuelles dans VMware Host Client

Les événements sont des enregistrements des actions qu'un utilisateur effectue sur une machine virtuelle. Lorsque vous créez une machine virtuelle dans VMware Host Client, vous pouvez afficher les événements associés à cette machine virtuelle.

### Conditions préalables

Privilège nécessaire : **Read only**.

### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez sur une machine virtuelle dans la liste.
- 3 Développez la machine virtuelle dans l'inventaire VMware Host Client et cliquez sur **Surveiller**.
- 4 Cliquez sur **Événements**.  
Une liste de tous les événements de machines virtuelles apparaît.
- 5 (Facultatif) Cliquez sur un événement de la liste pour afficher les détails de cet événement.
- 6 (Facultatif) Utilisez les contrôles de filtre sous la liste pour filtrer la liste.
- 7 (Facultatif) Cliquez sur l'en-tête d'une colonne pour trier la liste.

## Afficher les tâches des machines virtuelles dans VMware Host Client

Lorsque vous créez une machine virtuelle dans VMware Host Client, vous pouvez afficher toutes les tâches de cette machine virtuelle et les informations sur la cible des tâches, l'initiateur des tâches, la durée de file d'attente, l'heure de début des tâches, le résultat des tâches et la durée d'exécution des tâches.

### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez sur une machine virtuelle dans la liste.
- 3 Développez la machine virtuelle dans l'inventaire VMware Host Client et cliquez sur **Surveiller**.
- 4 Cliquez sur **Tâches**.
- 5 (Facultatif) Cliquez sur une tâche de la liste pour afficher les détails de cette tâche.

- 6 (Facultatif) Utilisez les contrôles de filtre sous la liste pour filtrer la liste.
- 7 (Facultatif) Cliquez sur l'en-tête d'une colonne pour trier la liste.

## Afficher l'explorateur de journaux de machines virtuelles dans VMware Host Client

Générez et surveillez les journaux pour l'hôte que vous gérez en utilisant VMware Host Client. Utilisez les journaux pour faire le diagnostic des différents problèmes de votre environnement hôte et les dépanner.

### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez sur une machine virtuelle dans la liste.
- 3 Développez la machine virtuelle dans l'inventaire VMware Host Client et cliquez sur **Surveiller**.
- 4 Cliquez sur **Journaux**.
- 5 (Facultatif) Cliquez sur **Générer un bundle de support** pour consolider tous les journaux pour le dépannage.
- 6 Cliquez avec le bouton droit sur un journal de la liste et sélectionnez **Ouvrir dans une nouvelle fenêtre** pour afficher le journal.

## Afficher les notifications des machines virtuelles dans VMware Host Client

Vous pouvez afficher les notifications des machines virtuelles et les informations sur les tâches associées que vous pouvez effectuer, pour les machines virtuelles que vous créez dans VMware Host Client.

### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez sur une machine virtuelle dans la liste.
- 3 Développez la machine virtuelle dans l'inventaire VMware Host Client et cliquez sur **Surveiller**.
- 4 Cliquez sur **Notifications**.  
Une liste contenant toutes les notifications de machines virtuelles apparaît.
- 5 (Facultatif) Cliquez sur une notification pour afficher les détails.
- 6 (Facultatif) Cliquez sur une notification et cliquez sur **Actions** pour afficher les tâches suggérées.

# Configurer le matériel d'une machine virtuelle dans VMware Host Client

# 5

Ce chapitre contient les rubriques suivantes :

- Configuration de CPU virtuel
- Configuration de la mémoire virtuelle
- Configuration de la machine virtuelle de réseau
- Configuration de disque virtuel
- Configuration des contrôleurs de machines virtuelles dans VMware Host Client
- Autre configuration de périphérique de machine virtuelle dans VMware Host Client
- Sécurisation des machines virtuelles dans VMware Host Client

## Configuration de CPU virtuel

Vous pouvez ajouter, modifier ou configurer des ressources de CPU pour améliorer les performances de machine virtuelle. Vous pouvez définir la plupart des paramètres de CPU lors de la création de machines virtuelles ou après l'installation du système d'exploitation invité. Quelques actions exigent la mise hors tension de la machine virtuelle avant de modifier les paramètres.

VMware utilise la terminologie suivante. Comprendre ces termes peut vous aider à planifier votre stratégie pour l'allocation de ressources de CPU.

### CPU

Le CPU, ou le processeur, est le composant d'un ordinateur qui exécute les tâches requises pour exécuter des applications d'ordinateur. Le CPU est l'élément principal qui exécute les fonctions de l'ordinateur. Les CPU contiennent des cœurs.

### Socket de CPU

Un socket de CPU est un connecteur physique sur une carte mère d'ordinateur qui se connecte à un seul CPU physique. Certaines cartes mères ont plusieurs sockets et peuvent se connecter à plusieurs processeurs multicoeurs (CPU).

### Cœur

Un cœur comporte une unité contenant un cache L1 et les unités fonctionnelles requises pour exécuter des applications. Les cœurs peuvent indépendamment exécuter des applications ou des threads. Un ou plusieurs cœurs peuvent exister sur une seule CPU.

### Partage des ressources

Les parts spécifient la priorité ou l'importance relative d'une machine virtuelle ou d'un pool de ressources. Si une machine virtuelle a deux fois plus de parts d'une ressource qu'une autre machine virtuelle, elle est autorisée à consommer deux fois plus de cette ressource quand les deux machines virtuelles sont en concurrence pour les ressources.

### Allocation des ressources

Vous pouvez changer les paramètres d'allocation de ressources de CPU, tels que les parts, la réservation et la limite lorsque la capacité des ressources disponibles ne répond pas à la demande. Par exemple, à la fin de l'année si la charge de travail de la comptabilité augmente, vous pouvez augmenter la réserve de pool de ressources pour la comptabilité.

### vSphere Virtual Symmetric Multiprocessing (Virtual SMP)

Virtual SMP ou vSphere Virtual Symmetric Multiprocessing est une fonctionnalité qui permet à une seule machine virtuelle d'avoir plusieurs processeurs.

## Limitations du CPU virtuel

Le nombre maximum de CPU virtuels que vous pouvez attribuer à une machine virtuelle est de 768. Le nombre maximum de CPU virtuels dépend du nombre de CPU logiques sur l'hôte et du type de système d'exploitation invité qui est installé sur la machine virtuelle.

Tenez comptes des limitations suivantes :

- Une machine virtuelle ne peut pas avoir un nombre de processeurs virtuels supérieur au nombre de cœurs logiques sur l'hôte. Le nombre de cœurs logiques est égal au nombre de cœurs physiques si l'hyperthreading est désactivé, ou est égal à deux fois ce nombre si l'hyperthreading est activé.
- Si une machine virtuelle active dispose, au maximum, de 128 CPU virtuels, vous ne pouvez pas utiliser l'ajout à chaud pour accroître le nombre de CPU virtuels. Pour dépasser cette limite, vous devez tout d'abord mettre hors tension la machine virtuelle. En revanche, si une machine virtuelle active a déjà plus de 128 CPU virtuels, vous pouvez utiliser l'ajout à chaud pour augmenter le nombre de CPU virtuels jusqu'à 768.
- Le nombre maximal de sockets de CPU virtuels dont une machine virtuelle peut disposer est de 128. Si vous souhaitez configurer une machine virtuelle avec plus de 128 CPU virtuels, vous devez utiliser des CPU virtuels multicœurs.
- Les systèmes d'exploitation invités ne prennent pas tous en charge Virtual SMP et les systèmes d'exploitation invités qui prennent en charge Virtual SMP peuvent prendre en charge moins de processeurs que ceux disponibles sur l'hôte. Pour plus d'informations sur la prise en charge de Virtual SMP, consultez le *Guide de compatibilité de VMware* à l'adresse <http://www.vmware.com/resources/compatibility>.

## Configuration de CPU multicœurs virtuelles

La prise en charge des CPU virtuels multicœurs VMware permet de contrôler le nombre de cœurs par socket virtuel dans une machine virtuelle. Cette possibilité permet aux systèmes d'exploitation présentant des restrictions de socket d'employer plus de cœurs de CPU hôtes, ce qui augmente les performances globales.

---

**Important** Lorsque vous configurez la machine virtuelle pour les paramètres de CPU virtuel multicœurs, vous devez vérifier que la configuration est conforme aux conditions du contrat CLUF du système d'exploitation invité.

---

L'utilisation des CPU virtuels multicœurs peut être utile quand vous exécutez des systèmes d'exploitation ou les applications qui peuvent tirer profit d'un nombre limité de sockets de CPU seulement.

Vous pouvez configurer une machine virtuelle compatible avec ESXi 7.0 Update 1 et versions ultérieures pour avoir jusqu'à 768 CPU virtuels. Une machine virtuelle ne peut pas avoir un nombre de CPU virtuels supérieur au nombre de CPU logiques sur l'hôte. Le nombre de CPU logiques correspond au nombre de cœurs de processeur physiques ou au double si l'hyperthreading est activé. Par exemple, si un hôte dispose de 128 CPU logiques, vous pouvez configurer la machine virtuelle pour 128 CPU virtuels.

Vous configurez la façon dont les CPU virtuels sont affectés en termes de cœurs et de cœurs par socket. Déterminez le nombre de CPU que la machine virtuelle doit avoir, puis sélectionnez le nombre de cœurs de chaque socket, selon que vous désirez un CPU monocœur, double cœur, triple cœur, etc. Votre choix détermine le nombre de sockets dont la machine virtuelle dispose.

Le nombre maximal de sockets de CPU virtuels dont une machine virtuelle peut disposer est de 128. Si vous souhaitez configurer une machine virtuelle avec plus de 128 CPU virtuels, vous devez utiliser des CPU virtuels multicœurs.

Pour plus d'informations sur les processeurs multicœurs, reportez-vous à la documentation *Gestion des ressources vSphere*.

## Changer le nombre de CPU virtuels

Une machine virtuelle compatible avec ESXi 7.0 Update 1 et versions ultérieures peut avoir jusqu'à 768 CPU virtuels. Vous pouvez modifier le nombre de CPU virtuels lorsque votre machine virtuelle est hors tension. Si l'ajout à chaud de CPU virtuel est activé, vous pouvez augmenter le nombre de CPU virtuels lorsque la machine virtuelle est en cours d'exécution.

L'ajout à chaud du CPU virtuel est pris en charge pour des machines virtuelles avec support multicore CPU et compatibles avec ESXi 5.0 et versions ultérieures. Lorsque la machine virtuelle est sous tension et que l'ajout à chaud de CPU est activé, vous pouvez ajouter à chaud des CPU virtuels à la machine virtuelle active. Vous pouvez ajouter uniquement des multiples du nombre de cœurs par socket.



Si une machine virtuelle dispose, au maximum, de 128 CPU virtuels, vous ne pouvez pas utiliser l'ajout à chaud pour accroître le nombre de CPU virtuels. Pour dépasser cette limite, vous devez tout d'abord mettre hors tension la machine virtuelle. En revanche, si une machine virtuelle a déjà plus de 128 CPU virtuels, vous pouvez utiliser l'ajout à chaud pour augmenter le nombre de CPU virtuels jusqu'à 768.

Le nombre maximal de sockets de CPU virtuels dont une machine virtuelle peut disposer est de 128. Si vous souhaitez configurer une machine virtuelle avec plus de 128 CPU virtuels, vous devez utiliser des CPU virtuels multicœurs.

---

**Important** Lorsque vous configurez la machine virtuelle pour les paramètres de CPU virtuel multicœurs, vous devez vérifier que la configuration est conforme aux conditions du contrat CLUF du système d'exploitation invité.

---

#### Conditions préalables

- Si l'ajout à chaud de CPU n'est pas activé, mettez hors tension la machine virtuelle avant d'ajouter des CPU virtuels.
- Pour ajouter à chaud des CPU multicœurs, vérifiez que la machine virtuelle est compatible avec les versions ESXi 5.0 et ultérieures.
- Vérifiez que vous disposez des privilèges **Machine virtuelle.Configuration.Modifier nombre de CPU**

#### Procédure

- 1 Cliquez avec le bouton droit de la souris sur une machine virtuelle dans l'inventaire et sélectionnez **Modifier les paramètres**.
- 2 Dans l'onglet **Matériel virtuel**, développez **CPU**.
- 3 Dans le menu déroulant **CPU**, sélectionnez le nombre de cœurs.
- 4 Dans le menu déroulant **Cœurs par socket**, sélectionnez le nombre de cœurs par socket et cliquez sur **OK**.

## Allouer des ressources CPU dans VMware Host Client

Pour gérer la demande de charge de travail, vous pouvez changer la quantité de ressources CPU allouées à une machine virtuelle en utilisant les partages, les réservations, et les paramètres de limites.

Une machine virtuelle a les paramètres définis par l'utilisateur suivants qui affectent son allocation de ressources de CPU.

#### Limite

Place une limite sur la consommation du temps CPU pour une machine virtuelle. Cette valeur est exprimée en MHz ou en GHz.

#### Réservation

Spécifie l'allocation minimum garantie pour une machine virtuelle. La réserve est exprimée en MHz ou en GHz.

## Parts

On accorde des parts CPU à chaque machine virtuelle. Plus une machine virtuelle a de parts, plus elle obtient souvent une part de temps d'un CPU quand il n'y a pas de temps d'inactivité de CPU. Les parts représentent une mesure relative pour allouer la capacité de CPU.

## Conditions préalables

Mettez la machine virtuelle hors tension.

## Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez avec le bouton droit sur une machine virtuelle de la liste et sélectionnez **Modifier les paramètres** dans le menu contextuel.
- 3 Sur l'onglet **Matériel virtuel**, développez **CPU** et allouez la capacité de CPU pour la machine virtuelle.

| Option      | Description  |
|-------------|--|
| Réservation | Affectation de CPU garantie pour cette machine virtuelle.  |
| Limite      | Limite maximale d'allocation de CPU de cette machine virtuelle. Sélectionnez <b>Illimité</b> pour spécifier aucune limite supérieure.  |
| Parts       | Parts de processeur de cette machine virtuelle par rapport au total du parent. Les machines virtuelles sœurs partagent des ressources selon leurs valeurs de part relatives limitées par la réservation et la limite. Sélectionnez <b>Bas</b> , <b>Normal</b> ou <b>Haut</b> , qui spécifie une valeur de part dans un rapport de 1:2:4 respectivement. Choisissez <b>Personnalisé</b> pour donner à chaque machine virtuelle un nombre spécifique de parts qui expriment une pondération proportionnelle. |

- 4 Cliquez sur **Enregistrer**.

## Configuration de la mémoire virtuelle

Vous pouvez ajouter, modifier ou configurer des ressources ou des options de mémoire de machine virtuelle pour améliorer les performances de machine virtuelle. Vous pouvez définir la plupart des paramètres de mémoire pendant la création de machine virtuelle ou après avoir installé le système d'exploitation client. Quelques actions exigent de mettre hors tension la machine virtuelle avant de modifier les paramètres.

Les paramètres des ressources de mémoire d'une machine virtuelle déterminent la quantité de mémoire de l'hôte allouée à la machine virtuelle. La taille de la mémoire du matériel virtuel détermine la quantité de mémoire disponible pour les applications qui s'exécutent dans la machine virtuelle. Une machine virtuelle ne peut pas bénéficier de plus de ressources de mémoire que sa taille de mémoire matérielle virtuelle configurée. Les hôtes ESXi limitent l'utilisation de ressources de mémoire à la quantité maximale utile à la machine virtuelle, de sorte que vous pouvez accepter les ressources de mémoire illimitées par défaut.

## Changer la configuration de mémoire

Vous pouvez configurer la mémoire allouée à une machine virtuelle afin d'améliorer ses performances.

La mémoire minimale est égale à 4 Mo pour les machines virtuelles qui utilisent le microprogramme BIOS. Les machines virtuelles qui utilisent un microprogramme EFI nécessitent au moins 96 Mo de RAM pour pouvoir se mettre sous tension.

La taille de mémoire maximale des machines virtuelles utilisant le microprogramme BIOS est 24 560 Go. Vous devez utiliser le microprogramme EFI pour les machines virtuelles dont la taille de mémoire est supérieure à 6 128 Go.

La taille maximale de la mémoire d'une machine virtuelle dépend de la mémoire physique de l'hôte ESXi et des paramètres de compatibilité de la machine virtuelle.

Si la mémoire de la machine virtuelle est supérieure à la taille de la mémoire de l'hôte, un échange se produit, ce qui peut avoir un fort impact sur les performances de la machine virtuelle. La taille maximale pour obtenir des performances optimales correspond au seuil au-dessus duquel la mémoire physique de l'hôte ESXi est insuffisante pour exécuter la machine virtuelle à sa vitesse maximale. Cette valeur fluctue quand les conditions sur l'hôte changent, par exemple, lorsque les machines virtuelles sont mises sous tension ou hors tension.

La taille de mémoire doit être un multiple de 4 Mo.

**Tableau 5-1. Mémoire maximale de machine virtuelle**

| Introduit dans la version hôte | Compatibilité de la machine virtuelle     | Taille maximale de mémoire |
|--------------------------------|---|----------------------------|
| ESXi 8.0                       | ESXi 8.0 et versions ultérieures          | 24 560 Go                  |
| ESXi 7.0 Update 3              | ESXi 7.0 Update 3 et versions ultérieures | 24 560 Go                  |
| ESXi 7.0 Update 2              | ESXi 7.0 Update 2 et versions ultérieures | 24 560 Go                  |
| ESXi 7.0 Update 1              | ESXi 7.0 Update 1 et versions ultérieures | 24 560 Go                  |
| ESXi 7.0                       | ESXi 7.0 et versions ultérieures          | 6 128 Go                   |
| ESXi 6.7 Update 2              | ESXi 6.7 Update 2 et versions ultérieures | 6 128 Go                   |
| ESXi 6.7                       | ESXi 6.7 et versions ultérieures          | 6 128 Go                   |

**Tableau 5-1. Mémoire maximale de machine virtuelle (suite)**

| Introduit dans la version hôte | Compatibilité de la machine virtuelle | Taille maximale de mémoire |
|--------------------------------|---------------------------------------|----------------------------|
| ESXi 6.5                       | ESXi 6.5 et versions ultérieures      | 6 128 Go                   |
| ESXi 6.0                       | ESXi 6.0 et versions ultérieures      | 4 080 Go                   |

La version hôte ESXi indique le début de la prise en charge pour l'augmentation de la taille de mémoire. Par exemple, la taille de la mémoire d'une machine virtuelle compatible avec ESXi 6.0 et versions ultérieures exécutée sur ESXi 6.5 est limitée à 4 080 Go.

### Conditions préalables

Vérifiez que vous disposez du privilège **Machine virtuelle.Configuration.Modifier la mémoire** sur la machine virtuelle.

### Procédure

- 1 Cliquez avec le bouton droit sur une machine virtuelle dans l'inventaire et sélectionnez **Modifier les paramètres**.
- 2 Dans l'onglet **Matériel virtuel**, développez **Mémoire** et modifiez la configuration de la mémoire.
  - a Dans la zone de texte **Mémoire**, indiquez la quantité de mémoire vive à affecter à la machine virtuelle.
  - b Indiquez si la mémoire est spécifiée en Mo, Go ou To.
- 3 Cliquez sur **OK**.

## Allouer les ressources en mémoire

Vous pouvez changer la quantité de ressources de mémoire allouée à une machine virtuelle en utilisant les paramètres de parts, de réservations et de limites. L'hôte détermine la quantité de mémoire physique appropriée à allouer aux machines virtuelles en fonction de ces paramètres. Vous pouvez allouer des parts élevées ou faibles à une machine virtuelle, en fonction de sa charge et de son état.

Les paramètres suivants définis par l'utilisateur affectent l'allocation des ressources mémoire d'une machine virtuelle.

### Limite

Place une limite sur la consommation de mémoire pour une machine virtuelle. Cette valeur est exprimée en mégaoctets.

### Réservation

Spécifie l'allocation minimum garantie pour une machine virtuelle. La réserve est exprimée en mégaoctets. S'il est impossible d'allouer cette réserve, la machine virtuelle ne s'activera pas.

## Parts

On accorde un certain nombre de parts mémoire à chaque machine virtuelle. Plus une machine virtuelle dispose de parts, plus elle reçoit de mémoire hôte. Les parts représentent une mesure relative pour allouer la capacité de mémoire. Pour plus d'informations sur les valeurs de part, reportez-vous à la documentation *Gestion des ressources vSphere*.

Impossible d'allouer à une machine virtuelle une réservation supérieure à sa mémoire configurée. Si vous allouez à une machine virtuelle une grande réservation, puis réduisez sa taille de mémoire configurée, la réservation est réduite pour correspondre à la nouvelle taille de mémoire configurée.

## Conditions préalables

Vérifiez si la machine virtuelle est désactivée.

## Procédure

- 1 Cliquez avec le bouton droit sur une machine virtuelle dans l'inventaire et sélectionnez **Modifier les paramètres**.
- 2 Sur l'onglet **Matériel virtuel**, développez la mémoire et allouez la capacité de mémoire pour la machine virtuelle.

| Option      | Description   |
|-------------|---|
| Réservation | Allocation de mémoire garantie pour cette machine virtuelle.  |
| Limite      | Limite maximale d'allocation de mémoire de la machine virtuelle.<br>Sélectionnez <b>Illimité</b> pour spécifier aucune limite supérieure.                                   |
| Parts       | Les valeurs <b>Bas</b> , <b>Normal</b> , <b>Haut</b> et <b>Personnalisé</b> sont comparées à la somme de toutes les parts de toutes les machines virtuelles sur le serveur. |

- 3 Cliquez sur **OK**.

## Changer les paramètres d'ajout de mémoire à chaud

L'ajout à chaud de mémoire vous permet d'ajouter des ressources en mémoire pour une machine virtuelle alors que celle-ci est sous tension.

L'activation de l'ajout à chaud de mémoire génère une surcharge de mémoire sur l'hôte ESXi pour la machine virtuelle.

## Conditions préalables

- Mettez la machine virtuelle hors tension.
- Vérifiez que la machine virtuelle dispose d'un système d'exploitation invité qui prend en charge les fonctionnalités d'ajout à chaud de mémoire.

- Vérifiez que la compatibilité de la machine virtuelle est ESXi 4.x et versions ultérieures.
- Vérifiez que VMware Tools est installé.

#### Procédure

- 1 Cliquez avec le bouton droit sur une machine virtuelle dans l'inventaire et sélectionnez **Modifier les paramètres**.
- 2 Sur l'onglet **Matériel virtuel**, développez **Mémoire** et sélectionnez **Activer** pour activer l'ajout de mémoire à la machine virtuelle alors qu'elle est sous tension.
- 3 Cliquez sur **OK**.

#### Résultats

Vous pouvez maintenant ajouter de la mémoire à une machine virtuelle même si celle-ci est sous tension.

---

**Note** L'ajout à chaud de mémoire à une machine virtuelle avec NVIDIA vGPU impose que l'hôte ESXi ait un emplacement vGPU libre.

---

## Ajout d'un périphérique NVDIMM à une machine virtuelle dans VMware Host Client

Ajoutez un périphérique NVDIMM virtuel à une machine virtuelle pour lui permettre d'utiliser une mémoire d'ordinateur non volatile ou persistante. Une mémoire non volatile (NVM), ou mémoire persistante (PMem), associe les taux de transfert de données élevés de la mémoire volatile à la persistance et à la résilience du stockage traditionnel. Le périphérique NVDIMM virtuel est un périphérique NVM virtuel capable de conserver les données stockées en cas de redémarrages ou de pannes des sources d'alimentation.

Les machines virtuelles consomment la ressource de PMem de l'hôte de deux façons : via un module virtuel de mémoire non volatile à double rangée de connexions (NVDIMM) ou via un disque virtuel à mémoire persistante.

Pour plus d'informations sur la mémoire persistante, reportez-vous à la section [Gestion de la mémoire persistante](#)

#### Conditions préalables

- Assurez-vous que le système d'exploitation invité de la machine virtuelle prend en charge la PMem.
- Vérifiez que la version du matériel virtuel est la version 14 ou une version ultérieure.
- Vérifiez que vous disposez du privilège **Banque de données.Allouer de l'espace**.
- Assurez-vous que l'hôte ou le cluster sur lequel réside la machine virtuelle dispose de ressources PMem disponibles.

## Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez avec le bouton droit sur une machine virtuelle de la liste et sélectionnez **Modifier les paramètres** dans le menu contextuel.
- 3 Sous l'onglet **Matériel virtuel**, cliquez sur **Ajouter un autre périphérique** et sélectionnez **NVDIMM** dans le menu déroulant.

Le périphérique NVDIMM apparaît dans la liste des périphériques du matériel virtuel. Chaque machine virtuelle peut avoir un maximum de 64 périphériques NVDIMM.

- 4 Configurer le périphérique NVDIMM récemment ajouté.
  - a Dans la liste de périphériques de matériel virtuel, développez **Nouveau NVDIMM**.
  - b Entrez la taille du nouveau périphérique NVDIMM.

---

**Note** Vous pouvez modifier la taille du périphérique NVDIMM ultérieurement. La machine virtuelle doit être mise hors tension.

---

- c Sélectionnez l'emplacement du contrôleur NVDIMM ou laissez celui par défaut.

- 5 Cliquez sur **Enregistrer** pour fermer l'assistant.

## Configuration de la machine virtuelle de réseau

Les fonctionnalités de mise en réseau de ESXi permettent aux machines virtuelles de communiquer entre elles, qu'elles appartiennent au même hôte ou à des hôtes différents, ainsi qu'avec des machines physiques.

Les fonctionnalités de mise en réseau permettent également de gérer les hôtes ESXi et fournissent la communication entre les services VMkernel tels que NFS, iSCSI, ou vSphere vMotion et le réseau physique. Quand vous configurez la mise en réseau pour une machine virtuelle, vous sélectionnez ou changez un type d'adaptateur, une connexion réseau, et s'il faut connecter le réseau lors de la mise sous tension de la machine virtuelle..

## Notions de base des adaptateurs réseau

Quand vous configurez une machine virtuelle, vous pouvez ajouter des adaptateurs réseau et spécifier le type d'adaptateur.

### Types d'adaptateur réseau

Les types d'adaptateurs réseau qui sont disponibles dépendent des facteurs suivants :

- La compatibilité de la machine virtuelle, qui dépend de l'hôte qui l'a créée ou récemment mise à niveau.
- Si la compatibilité de la machine virtuelle a été mise à niveau avec la version la plus récente de l'hôte actuel.

- Le système d'exploitation client.

Les NIC actuellement prises en charge ne sont pas les mêmes entre un environnement sur site et VMware Cloud on AWS. Les types de NIC suivants sont pris en charge dans un déploiement sur site :

### **E1000E**

Version émulée de la carte réseau Intel 82574 Gigabit Ethernet. E1000E est l'adaptateur par défaut pour Windows 8 et Windows Server 2012.

### **E1000**

Version émulée de la carte réseau Intel 82545EM Gigabit Ethernet, avec les pilotes disponibles dans les derniers systèmes d'exploitation clients, y compris Windows XP et les versions ultérieures et Linux versions 2.4.19 et les versions ultérieures.

### **Flexible**

S'identifie elle-même comme adaptateur Vlanx lorsqu'une machine virtuelle démarre, mais s'initialise elle-même et fonctionne comme carte Vlanx ou VMXNET en fonction du pilote qui l'initialise. Avec VMware Tools installé, le pilote VMXNET remplace l'adaptateur Vlanx par l'adaptateur VMXNET hautes performances.

### **Vlanx**

Version émulée de la carte réseau AMD 79C970 PCnet32 LANCE, une ancienne carte réseau 10 Mbit/s avec des pilotes disponibles dans les anciens systèmes d'exploitation invités 32 bits. Une machine virtuelle configurée avec cet adaptateur réseau peut utiliser immédiatement son réseau.

### **VMXNET**

Optimisé au niveau des performances dans une machine virtuelle et n'a aucun équivalent physique. Étant donné que les fournisseurs de systèmes d'exploitation ne fournissent pas les pilotes de cette carte, vous devez installer VMware Tools pour pouvoir disposer d'un pilote pour l'adaptateur réseau VMXNET.

### **VMXNET 2 (amélioré)**

Basé sur l'adaptateur VMXNET, mais fournit des fonctions hautes performances communément utilisées sur les réseaux actuels, telles que trames Jumbo et déchargements matériels. VMXNET 2 (amélioré) est disponible uniquement pour certains systèmes d'exploitation invités sur ESX/ESXi 3.5 et les versions ultérieures.

### **VMXNET 3**

Carte réseau paravirtualisée, conçue pour améliorer les performances. VMXNET 3 offre toutes les fonctions de VMXNET 2 et de nouvelles fonctions, telles que la prise en charge de plusieurs files d'attente (nommée également Mise à l'échelle côté réception dans Windows), les déchargements IPv6 et la distribution des interruptions MSI/MSI-X. VMXNET 3 n'est pas associé à VMXNET ni à VMXNET 2.



## PVRDMA

Carte réseau paravirtualisée prenant en charge l'accès mémoire direct à distance (RDMA) entre les machines virtuelles via l'API verbe OFED. Toutes les machines virtuelles doivent disposer d'un périphérique PVRDMA et doivent être connectées à un commutateur distribué. PVRDMA prend en charge VMware vSphere vMotion et la technologie des snapshots. Elle est disponible sur les machines virtuelles équipées de la version matérielle 13 et du noyau du système d'exploitation invité Linux 4.6 ou version ultérieure.

Pour plus d'informations sur l'affectation d'un adaptateur réseau PVRDMA à une machine virtuelle, reportez-vous à la documentation *Mise en réseau vSphere*.

## Relais SR-IOV

Représentation d'une fonction virtuelle (VF) sur une carte réseau physique avec prise en charge de SR-IOV. La machine virtuelle et l'adaptateur physique échangent des données sans utiliser VMkernel comme intermédiaire. Ce type d'adaptateur convient aux machines virtuelles dans lesquelles la latence risque de provoquer une panne ou qui nécessitent davantage de ressources CPU.

Le relais SR-IOV est disponible dans ESXi 6.0 et les versions ultérieures pour les systèmes d'exploitation Red Hat Enterprise Linux 6 (et versions ultérieures) et Windows Server 2008 R2 avec SP2. Une version de système d'exploitation peut contenir un pilote VF par défaut pour certaines cartes réseau, mais pour les autres versions, vous devez le télécharger et l'installer à partir d'un site mis à disposition par le fournisseur de la carte réseau ou de l'hôte.

Pour plus d'informations sur l'affectation d'un adaptateur réseau de relais SR-IOV à une machine virtuelle, reportez-vous à la documentation *Mise en réseau vSphere*.

Pour les considérations relatives à la compatibilité des adaptateurs réseau, reportez-vous au *Guide de compatibilité VMware* à l'adresse <http://www.vmware.com/resources/compatibility>.

## Adaptateurs réseau hérités et versions de matériel virtuel ESXi

Les types d'adaptateurs réseau pour toutes les machines virtuelles héritées dépendent des adaptateurs disponibles et compatibles pour le système d'exploitation client et de la version du matériel virtuel sur lequel la machine virtuelle avait été créée.

Si vous ne mettez pas à niveau une machine virtuelle afin d'utiliser une version de matériel virtuel, les paramètres de votre adaptateur restent inchangés. Si vous mettez à niveau votre machine virtuelle pour bénéficier du matériel virtuel plus récent, les paramètres de l'adaptateur par défaut seront probablement modifiés afin d'être compatibles avec le système d'exploitation client et le matériel de l'hôte mis à niveau.

Pour identifier les adaptateurs réseau disponibles dans le système d'exploitation invité pris en charge pour une version donnée de vSphere ESXi, reportez-vous au *Guide de compatibilité VMware* à l'adresse <http://www.vmware.com/resources/compatibility>.

## Adaptateurs réseau et machines virtuelles héritées

Les machines virtuelles héritées sont des machines virtuelles qui sont prises en charge par le produit utilisé, mais qui ne sont pas d'actualité pour ce produit. Les types d'adaptateurs réseau pour toutes les machines virtuelles héritées dépendent des adaptateurs disponibles et compatibles pour le système d'exploitation client et de la version du matériel virtuel sur lequel la machine virtuelle avait été créée.

Si vous ne mettez pas à niveau une machine virtuelle pour qu'elle corresponde à une nouvelle version d'un hôte ESXi, les paramètres d'adaptateur ne changent pas. Si vous mettez à niveau votre machine virtuelle pour bénéficier du matériel virtuel plus récent, les paramètres de l'adaptateur par défaut seront probablement modifiés afin d'être compatibles avec le système d'exploitation client et le matériel de l'hôte mis à niveau.

Pour identifier les adaptateurs réseau disponibles dans le système d'exploitation invité pris en charge pour une version donnée de vSphere ESXi, reportez-vous au *Guide de compatibilité VMware* à l'adresse <http://www.vmware.com/resources/compatibility>.

## Modifier la configuration de l'adaptateur réseau virtuel dans VMware Host Client

Vous pouvez configurer le paramètre de connexion à la mise sous tension, l'adresse MAC et la connexion réseau de l'adaptateur réseau virtuel pour une machine virtuelle.

### Conditions préalables

Privilèges requis :

- **Machine virtuelle.Configuration.Modifier les paramètres de périphérique** pour la modification de l'adresse et du réseau MAC.
- **Machine virtuelle.Interaction.Connexion de périphérique** pour la modification de **Connexion** et de **Connexion à la mise sous tension**.
- **Réseau.Attribuer un réseau**

### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez avec le bouton droit sur une machine virtuelle de la liste et sélectionnez **Modifier les paramètres** dans le menu contextuel.
- 3 Cliquez sur l'onglet **Matériel virtuel** et sélectionnez l'adaptateur réseau (NIC) approprié dans la liste de matériel.
- 4 (Facultatif) Pour connecter la carte d'interface réseau virtuelle quand la machine virtuelle est sous tension, sélectionnez **Connexion lors de la mise sous tension**.
- 5 (Facultatif) Sélectionnez le type d'adaptateur dans le menu déroulant **Type d'adaptateur**.

- 6 Sélectionnez une option pour la configuration d'adresse MAC.

| Option      | Description                                       |
|-------------|---|
| Automatique | vSphere attribue automatiquement une adresse MAC. |
| Manuel      | Entrez l'adresse MAC à utiliser.                  |

- 7 Cliquez sur **Enregistrer**.

## Ajouter une carte réseau à une machine virtuelle dans VMware Host Client

Quand vous ajoutez un adaptateur réseau (NIC) à une machine virtuelle, vous devez sélectionner le type d'adaptateur, la connexion réseau et indiquer si le périphérique doit se connecter quand la machine virtuelle est mise sous tension.

### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez avec le bouton droit sur une machine virtuelle de la liste et sélectionnez **Modifier les paramètres** dans le menu contextuel.
- 3 Cliquez sur l'onglet **Matériel virtuel** et cliquez sur **Ajouter un adaptateur réseau**.
- 4 Dans le panneau de connexion réseau, sélectionnez soit un réseau avec une étiquette spécifiée ou un réseau hérité.
- 5 (Facultatif) Pour configurer la carte réseau virtuelle de manière à ce qu'elle se connecte quand la machine virtuelle est sous tension, sélectionnez **Connexion à la mise sous tension**.
- 6 Cliquez sur **Enregistrer**.

## Configuration de disque virtuel

Vous pouvez ajouter des disques virtuels haute capacité aux machines virtuelles et ajouter de l'espace aux disques existants, même lorsque la machine virtuelle est en cours d'exécution. Vous pouvez définir la plupart des paramètres de disque virtuel pendant la création de machine virtuelle ou après avoir installé le système d'exploitation invité.

Vous pouvez stocker des données de machine virtuelle sur un nouveau disque virtuel, un disque virtuel existant, ou un LUN SAN mappé. Un disque virtuel est reconnu comme un disque dur unique par le système d'exploitation invité. Le disque virtuel se compose d'un ou plusieurs fichiers sur le système de fichiers hôte. Vous pouvez copier ou déplacer des disques virtuels sur les mêmes hôtes ou entre les hôtes.

Pour les machines virtuelles fonctionnant sur un hôte ESXi, vous pouvez stocker les données de machine virtuelle directement dans un LUN SAN plutôt que de les stocker dans un fichier disque virtuel. Cette option est utile si vous exécutez dans vos machines virtuelles des applications qui doivent détecter les caractéristiques physiques du périphérique de stockage. Le mappage d'un LUN de réseau SAN vous permet également d'utiliser des commandes SAN existantes pour gérer le stockage pour le disque.

Lorsque vous mappez un LUN à un volume VMFS, vCenter Server ou l'hôte ESXi crée un fichier de mappage de périphérique brut (RDM) renvoyant au LUN brut. L'encapsulation des informations de disque dans un fichier permet à vCenter Server ou à l'hôte ESXi de verrouiller le LUN de sorte qu'une seule machine virtuelle peut écrire dessus. Ce fichier porte l'extension `.vdmk`, mais le fichier contient uniquement des informations de disque qui décrivent le mappage à l'unité LUN sur le système ESXi. Les données réelles sont stockées sur le LUN. Vous ne pouvez pas déployer de machine virtuelle à partir d'un modèle et stocker ses données sur un LUN. Vous pouvez stocker ses données seulement dans un fichier-disque virtuel.

La quantité d'espace disponible dans la banque de données change continuellement. Assurez-vous de conserver suffisamment d'espace pour la création de la machine virtuelle et pour d'autres opérations de la machine virtuelle, telles que la croissance des fichiers fragmentés, des snapshots, etc. Pour plus d'informations sur l'utilisation de l'espace de la banque de données par type de fichier, reportez-vous à la documentation *Surveillance et performances vSphere*.

Le provisionnement dynamique vous permet de créer des fichiers fragmentés avec des blocs alloués au premier accès, ce qui permet de surprovisionner la banque de données. Les fichiers fragmentés peuvent continuer de croître et de remplir la banque de données. Si la banque de données manque d'espace disque alors que la machine virtuelle est en cours d'exécution, cette dernière peut s'arrêter de fonctionner.

## À propos des règles de provisionnement des disques virtuels

Lorsque vous effectuez certaines opérations de gestion de machines virtuelles, vous pouvez spécifier une stratégie de provisionnement pour le fichier de disque virtuel. Ces opérations sont notamment la création d'un disque virtuel, le clonage d'une machine virtuelle vers un modèle ou la migration d'une machine virtuelle.

Les banques de données NFS avec l'accélération matérielle et les banques de données VMFS prennent en charge les règles de provisionnement de disque suivantes. Dans les banques de données NFS qui ne prennent pas en charge l'accélération matérielle, seul le format dynamique est disponible.

Vous pouvez utiliser Storage vMotion ou Storage vMotion entre hôtes pour convertir les disques virtuels d'un format dans un autre.

### Provisionnement statique mis à zéro en différé

Crée un disque virtuel au format épais par défaut. L'espace nécessaire pour le disque virtuel est alloué lors de la création du disque. Les données qui demeurent sur le périphérique physique ne sont pas effacées pendant la création. Elles seront mises à zéro plus tard sur demande, à la première écriture de la machine virtuelle. Les machines virtuelles ne lisent pas les données périmées du disque physique.

### Provisionnement statique immédiatement mis à zéro

Un type de disque virtuel statique qui prend en charge des fonctions telles que Fault Tolerance. L'espace nécessaire au disque virtuel est alloué lors de la création. Contrairement au format de provisionnement statique mis à zéro en différé, les données restantes sur le périphérique physique seront remises à zéro lorsque le disque virtuel sera créé. La création de disques virtuels dans ce format peut être plus longue que pour d'autres types de disques. L'augmentation de la taille d'un disque virtuel immédiatement mis à zéro génère un temps de latence important pour la machine virtuelle.

### Provisionnement dynamique

Employez ce format pour économiser de l'espace de stockage. Pour le disque dynamique, vous fournissez la quantité d'espace de banque de données dont le disque a besoin, en fonction de la valeur que vous avez indiquée pour la taille de disque virtuel. Toutefois, le disque dynamique démarre avec un petit espace et il utilise au début uniquement l'espace de banque de données dont il a besoin pour ses opérations initiales. 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.

Le provisionnement dynamique est la méthode la plus rapide pour créer un disque virtuel, car il crée un disque qui comprend uniquement les informations d'en-tête. Il n'alloue pas ou ne met pas à zéro les blocs de stockage. Les blocs de stockage sont alloués et mis à zéro au premier accès.

---

**Note** Si un disque virtuel est compatible avec des solutions de mise en cluster, telles que Fault Tolérance, ne créez pas un disque fin.

---

## Changer la configuration d'un disque virtuel dans VMware Host Client

Si vous manquez d'espace disque, vous pouvez augmenter la taille du disque. Vous pouvez changer le nœud de périphérique virtuel et le mode de persistance de la configuration du disque virtuel d'une machine virtuelle.

### Conditions préalables

Mettez la machine virtuelle hors tension.

Vérifiez que vous disposez des privilèges suivants :

- **Machine virtuelle.Configuration.Modifier les paramètres de périphérique** sur la machine virtuelle.
- **Machine virtuelle.Configuration.Développer disque virtuel** sur la machine virtuelle.
- **Banque de données.Allouer de l'espace** sur la banque de données.

#### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez avec le bouton droit sur une machine virtuelle de la liste et sélectionnez **Modifier les paramètres** dans le menu contextuel.
- 3 Sous l'onglet **Matériel virtuel**, développez le disque dur pour afficher toutes les options du disque.
- 4 (Facultatif) Pour changer la taille du disque, entrez une nouvelle valeur dans la zone de texte et sélectionnez les unités dans le menu déroulant.
- 5 (Facultatif) Pour modifier la façon dont les disques sont affectés par les snapshots, sélectionnez un mode de disque dans le menu déroulant **Mode Disque**.

| Option                             | Description   |
|------------------------------------|---|
| <b>Dépendant</b>                   | Les disques dépendants sont inclus dans les snapshots.  |
| <b>Indépendant - Permanent</b>     | Les disques en mode persistant se comportent comme des disques normaux sur votre ordinateur physique. Toutes les données écrites sur un disque en mode persistant sont écrites de manière permanente sur le disque.   |
| <b>Indépendant - Non permanent</b> | Les modifications des disques en mode de non-persistant sont supprimées lorsque vous mettez hors tension la machine virtuelle ou la réinitialisez. Avec le mode non persistant, vous pouvez redémarrer la machine virtuelle avec un disque virtuel dans le même état chaque fois. Les modifications des disques sont écrites et lues dans un fichier journal qui est supprimé lorsque vous mettez sous tension ou réinitialisez la machine virtuelle. |

- 6 Cliquez sur **Enregistrer**.

## Ajouter un nouveau disque dur standard à une machine virtuelle dans VMware Host Client

Vous pouvez ajouter un disque dur virtuel à une machine virtuelle existante, ou vous pouvez ajouter un disque dur lorsque vous personnalisez le matériel de la machine virtuelle pendant le processus de création de la machine virtuelle. Par exemple, vous pouvez avoir besoin d'un espace disque supplémentaire pour une machine virtuelle existante avec une lourde charge de travail. Pendant la création de la machine virtuelle, vous souhaitez peut-être ajouter un disque dur préconfiguré en tant que disque de démarrage.

## Conditions préalables

- Vous devez être familiarisé avec les options de configuration et les mises en garde concernant l'ajout de disques durs virtuels. Reportez-vous à la section [Configuration de disque virtuel](#).
- Avant d'ajouter des disques d'une capacité supérieure à 2 To à une machine virtuelle, reportez-vous à *Administration d'une machine virtuelle vSphere*.
- Vérifiez que vous disposez du privilège **Machine virtuelle.Configuration.Ajouter un nouveau disque** sur le dossier ou la banque de données de destination.

Mettez la machine virtuelle hors tension.

## Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez avec le bouton droit sur une machine virtuelle de la liste et sélectionnez **Modifier les paramètres** dans le menu contextuel.
- 3 (Facultatif) Pour supprimer un disque dur existant, déplacez votre pointeur sur le disque et cliquez sur l'icône **Supprimer (X)**.

Le disque est retiré de la machine virtuelle. Si d'autres machines virtuelles partagent le disque, les fichiers du disque ne sont pas supprimés.

- 4 Sur l'onglet **Matériel virtuel**, sélectionnez **Ajouter un disque dur** et sélectionnez **Nouveau disque dur standard** dans le menu déroulant.

Le disque dur figure dans la liste des périphériques du matériel virtuel.

- 5 Développez **Nouveau disque dur**.
- 6 (Facultatif) Entrez une valeur pour la taille du disque dur et sélectionnez l'unité dans le menu déroulant.
- 7 Sélectionnez l'emplacement de la banque de données où vous voulez stocker les fichiers de la machine virtuelle.

## 8 Sélectionnez le format du disque de la machine virtuelle.

| Option   | Description   |
|--|---|
| <b>Provisionnement statique mis à zéro en différé</b>    | Créez un disque virtuel au format statique par défaut. L'espace nécessaire au disque virtuel est alloué lors de la création. Aucune donnée restant sur le périphérique physique n'est effacée lors de la création. Elles sont mises à zéro sur demande lors de la première écriture effectuée par la machine virtuelle.   |
| <b>Provisionnement statique immédiatement mis à zéro</b> | Créez un disque statique qui prend en charge des fonctions de mise en cluster, telles que Fault Tolerance. L'espace nécessaire au disque virtuel est alloué lors de la création. Contrairement au format plat, les données qui restent sur le périphérique physique sont mises à zéro lors de la création. La création de disques à ce format peut être plus longue que pour d'autres types de disques. |
| <b>Provisionnement dynamique</b>                         | Utilisez le format de provisionnement dynamique. Au départ, un disque à provisionnement dynamique utilise seulement la quantité d'espace de banque de données dont le disque a besoin initialement. Si le disque dynamique a besoin ultérieurement de davantage d'espace, il pourra croître jusqu'à la capacité maximale qui lui est allouée.   |

## 9 Dans le menu déroulant **Parts**, sélectionnez une valeur pour les parts à allouer au disque virtuel.

Les parts correspondent à une valeur qui représente la mesure relative pour contrôler la bande passante du disque. Les valeurs Basses, Normales, Hautes et Personnalisées sont comparées à la somme de toutes les parts de toutes les machines virtuelles sur l'hôte.

## 10 Si vous avez sélectionné **Personnalisée**, entrez un nombre de parts dans la zone de texte.

## 11 Dans la zone **Limite - IOPS**, entrez la limite maximale de ressources de stockage à allouer à la machine virtuelle ou sélectionnez **Illimitée**.

Cette valeur est le nombre maximal d'opérations E/S par seconde alloué au disque virtuel.

## 12 Acceptez le paramètre par défaut ou sélectionnez un autre nœud du périphérique virtuel.

Dans la plupart des cas, vous pouvez accepter le nœud du périphérique par défaut. Pour un disque dur, l'utilisation d'un nœud de périphérique autre que celui par défaut facilite le contrôle de l'ordre de démarrage et l'utilisation de différents types de contrôleurs SCSI. Par exemple, vous pouvez vouloir démarrer depuis un contrôleur LSI Logic et partager un disque de données avec une autre machine virtuelle qui utilise un contrôleur Buslogic avec le partage de bus activé.



**13** (Facultatif) Sélectionnez un mode de disque.

| Option                      | Description   |
|-----------------------------|---|
| Dépendant                   | Les disques dépendants sont inclus dans les snapshots.  |
| Indépendant - Permanent     | Les disques en mode permanent se comportent comme des disques d'ordinateurs physiques conventionnels. Toutes les données écrites sur un disque en mode persistant sont écrites de manière permanente sur le disque.   |
| Indépendant - Non permanent | Les modifications des disques en mode de non-persistant sont supprimées lorsque vous mettez hors tension la machine virtuelle ou la réinitialisez. Le disque virtuel retrouve le même état à chaque fois que vous redémarrez la machine virtuelle. Les modifications des disques sont écrites et lues dans un fichier journal de rétablissement qui est supprimé lorsque vous mettez hors tension ou réinitialisez. |

**14** Cliquez sur **Enregistrer**.

## Ajouter un disque dur existant à une machine virtuelle dans VMware Host Client

Vous pouvez ajouter un disque dur virtuel existant à une machine virtuelle si vous personnalisez le matériel de la machine virtuelle pendant le processus de création de la machine virtuelle ou après la création de la machine virtuelle. Par exemple, vous souhaitez peut-être ajouter un disque dur existant préconfiguré en tant que disque de démarrage.

Pendant la création de la machine virtuelle, un disque dur et un contrôleur SCSI ou SATA sont ajoutés à la machine virtuelle par défaut, en fonction du système d'exploitation invité que vous sélectionnez. Si ce disque ne répond pas à vos besoins, vous pouvez le supprimer et ajouter un disque dur existant à la fin du processus de création.

### Conditions préalables

- Vérifiez que vous êtes familiarisé avec le comportement du contrôleur et des nœuds de périphériques virtuels pour différentes configurations de disque dur virtuel.
- Vérifiez que vous disposez du privilège **Machine virtuelle.Configuration.Ajouter un disque existant** sur le dossier ou la banque de données de destination.

Mettez la machine virtuelle hors tension.

### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez avec le bouton droit sur une machine virtuelle de la liste et sélectionnez **Modifier les paramètres** dans le menu contextuel.
- 3 Sur l'onglet **Matériel virtuel**, sélectionnez **Ajouter un disque dur** et sélectionnez **Disque dur existant** dans le menu déroulant.

- 4 (Facultatif) Pour supprimer un disque dur existant, déplacez votre pointeur sur le disque et cliquez sur l'icône **Supprimer (X)**.

Le disque est retiré de la machine virtuelle. Si d'autres machines virtuelles partagent le disque, les fichiers du disque ne sont pas supprimés.

- 5 Dans la colonne Banques de données, développez une banque de données, sélectionnez un dossier de machine virtuelle, puis sélectionnez le disque à ajouter.

Le fichier disque apparaît dans la colonne Contenu. Le menu **Type de fichier** affiche les types de fichiers de compatibilité pour ce disque.

- 6 Cliquez sur **Sélectionner** et cliquez sur **Enregistrer** pour ajouter le disque dur existant.

## Ajouter un disque à mémoire persistante dans Host Client

Vous pouvez ajouter un disque dur virtuel à une machine virtuelle existante, ou vous pouvez ajouter un disque dur lorsque vous personnalisez le matériel de la machine virtuelle pendant le processus de création de la machine virtuelle. Par exemple, vous pouvez avoir besoin d'un espace disque supplémentaire pour une machine virtuelle existante avec une lourde charge de travail. Pendant la création de la machine virtuelle, vous souhaitez peut-être ajouter un disque dur préconfiguré en tant que disque de démarrage.

Pendant la création de la machine virtuelle, un disque dur et un contrôleur SCSI ou SATA sont ajoutés à la machine virtuelle par défaut, en fonction du système d'exploitation invité que vous sélectionnez. Si ce disque ne répond pas à vos besoins, vous pouvez le supprimer et ajouter un disque dur existant à la fin du processus de création.

### Conditions préalables

- Vous devez être familiarisé avec les options de configuration et les mises en garde concernant l'ajout de disques durs virtuels. Reportez-vous à la section [Configuration de disque virtuel](#).
- Avant d'ajouter des disques d'une capacité supérieure à 2 To à une machine virtuelle, reportez-vous à *Administration d'une machine virtuelle vSphere*.
- Vérifiez que vous disposez du privilège **Machine virtuelle.Configuration.Ajouter un nouveau disque** sur le dossier ou la banque de données de destination.

Mettez la machine virtuelle hors tension.

### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez avec le bouton droit sur une machine virtuelle de la liste et sélectionnez **Modifier les paramètres** dans le menu contextuel.

- 3 Sur l'onglet **Matériel virtuel**, sélectionnez **Ajouter un disque dur** et sélectionnez **Nouveau disque à mémoire persistante** dans le menu déroulant.

Le disque dur figure dans la liste des périphériques du matériel virtuel. Par défaut, le disque est stocké sur la banque de données PMem locale au niveau de l'hôte, et vous ne pouvez pas modifier la banque de données.

- 4 (Facultatif) Configurez les paramètres pour le nouveau disque dur et cliquez sur **Enregistrer** pour fermer l'assistant.
  - a Développez **Nouveau disque dur**.
  - b Entrez une valeur pour la taille du disque dur et sélectionnez l'unité dans le menu déroulant.

---

**Note** Tous les disques durs à mémoire persistante et les modules NVDIMM que vous ajoutez à la machine virtuelle partagent les mêmes ressources PMem. Par conséquent, vous devez ajuster la taille des périphériques à mémoire persistante récemment ajoutés en fonction de la quantité de PMem disponible pour l'hôte. Si une partie de la configuration nécessite une attention, l'assistant vous en avertit.

---

- c Dans le menu déroulant **Parts**, sélectionnez une valeur pour les parts à allouer au disque virtuel.

Les parts correspondent à une valeur qui représente la mesure relative pour contrôler la bande passante du disque. Les valeurs Basses, Normales, Hautes et Personnalisées sont comparées à la somme de toutes les parts de toutes les machines virtuelles sur l'hôte.

- d Dans le menu déroulant **Emplacement du contrôleur**, sélectionnez l'emplacement du contrôleur que le nouveau disque dur utilise.
  - e Sélectionnez un mode de disque.

| Option                      | Description   |
|-----------------------------|---|
| Dépendant                   | Les disques dépendants sont inclus dans les snapshots.  |
| Indépendant - Permanent     | Les disques en mode permanent se comportent comme des disques d'ordinateurs physiques conventionnels. Toutes les données écrites sur un disque en mode persistant sont écrites de manière permanente sur le disque.   |
| Indépendant - Non permanent | Les modifications des disques en mode de non-persistant sont supprimées lorsque vous mettez hors tension la machine virtuelle ou la réinitialisez. Le disque virtuel retrouve le même état à chaque fois que vous redémarrez la machine virtuelle. Les modifications des disques sont écrites et lues dans un fichier journal de rétablissement qui est supprimé lorsque vous mettez hors tension ou réinitialisez. |

## Utiliser les partages de disque pour définir la priorité des machines virtuelles dans VMware Host Client

Vous pouvez changer les ressources en disque pour une machine virtuelle. Si plusieurs machines virtuelles accèdent à la même banque de données VMFS et au même numéro d'unité logique (LUN), utilisez les partages de disque pour définir la priorité du niveau d'accès que les machines virtuelles ont aux ressources. Les parts de disque distinguent les machines virtuelles à haute priorité et à basse priorité.

Vous pouvez allouer la bande passante d'entrée-sortie de l'hôte aux disques durs virtuels d'une machine virtuelle. Vous ne pouvez pas mettre en commun des entrées-sorties de disque sur un cluster.

La valeur des partages représente la mesure relative pour la bande passante de contrôle de disque à toutes les machines virtuelles.

Les parts de disque sont uniquement utiles au sein d'un hôte défini. Les parts assignées aux machines virtuelles sur un hôte n'exercent aucun effet sur des machines virtuelles sur d'autres hôtes.

Vous pouvez sélectionner une limite d'IOP, qui définit une limite supérieure pour les ressources de stockage allouées à une machine virtuelle. Les IOPS représentent le nombre d'opérations d'entrée/sortie par seconde.

### Conditions préalables

Mettez la machine virtuelle hors tension.

### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez avec le bouton droit sur une machine virtuelle de la liste et sélectionnez **Modifier les paramètres** dans le menu contextuel.
- 3 Dans l'onglet **Matériel virtuel**, développez le disque dur pour afficher les options du disque.
- 4 Dans le menu déroulant **Parts**, sélectionnez une valeur pour les parts à allouer à la machine virtuelle.
- 5 Si vous avez sélectionné **Personnalisée**, entrez un nombre de parts dans la zone de texte.
- 6 Dans la zone de texte **Limite - IOPS**, entrez la limite maximale de ressources de stockage à allouer à la machine virtuelle ou sélectionnez **Illimitée**.
- 7 Cliquez sur **Enregistrer**.

## Configuration des contrôleurs de machines virtuelles dans VMware Host Client

Dans VMware Host Client, vous pouvez ajouter différents contrôleurs à des machines virtuelles, comme des contrôleurs USB, des contrôleurs SCSI, des contrôleurs Paravirtual SCSI et des

contrôleurs SATA. Vous pouvez également modifier la configuration de partage des bus SCSI et le type de contrôleur SCSI.

## Ajouter un contrôleur USB à une machine virtuelle

Pour prendre en charge le relais USB à partir d'un hôte ESXi ou d'un ordinateur client vers une machine virtuelle, vous pouvez ajouter un contrôleur USB à la machine virtuelle.

Dans vSphere Client, vous pouvez ajouter un contrôleur xHCI et un contrôleur EHCI+UHCI. De la version matérielle 11 à la version matérielle 16, le nombre de ports de concentrateur racine par contrôleur xHCI est huit (quatre ports logiques USB 3.1 SuperSpeed et quatre ports logiques USB 2.0). Dans la version matérielle 17, huit ports de concentrateur racine sont pris en charge par le contrôleur xHCI (quatre ports logiques USB 3.1 SuperSpeedPlus et quatre ports logiques USB 2.0).

Les conditions d'ajout d'un contrôleur dépendent de la version du périphérique, du type de relais (hôte ou ordinateur client) et du système d'exploitation invité.

**Tableau 5-2. Prise en charge de contrôleur USB**

| Type de contrôleur | Version de périphérique USB prise en charge | Pris en charge pour le relais d'un hôte ESXi vers une machine virtuelle | Pris en charge pour le relais d'un ordinateur client vers une machine virtuelle  |
|--------------------|---|---|--|
| EHCI+UHCI          | 2.0 et 1.1                                  | Oui   | Oui  |
| xHCI               | 3.1, 2.0 et 1.1                             | Oui<br>Périphériques USB 3.1, 2.0 et 1.1 uniquement.                    | Oui<br>Windows 8 ou version ultérieure, Windows Server 2012 et versions ultérieures, ou un système d'exploitation invité Linux avec un noyau 2.6.35 ou version ultérieure. |

Pour les systèmes Mac OS X, le contrôleur EHCI+UHCI est activé par défaut et il est requis pour accéder à une souris et à un clavier USB.

Pour les machines virtuelles disposant de systèmes d'exploitation invités Windows ou Linux, vous pouvez ajouter un ou deux contrôleurs de différents types. Vous ne pouvez pas ajouter deux contrôleurs du même type.

Pour le relais USB d'un hôte ESXi vers une machine virtuelle, l'arbitre USB peut contrôler jusqu'à 15 contrôleurs USB. Si votre système comporte plus de 15 contrôleurs et que vous y connectez des périphériques USB, la machine virtuelle n'y a pas accès.

### Conditions préalables

- Vérifiez que les hôtes ESXi disposent du matériel et des modules de contrôleur USB prenant en charge les périphériques USB 3.1, 2.0 et 1.1.
- Vérifiez que les ordinateurs clients disposent du matériel et des modules de contrôleur USB qui prennent en charge les périphériques USB 3.1 ou 2.0 et 1.1 présents.

- Pour utiliser le contrôleur xHCI sur un invité Linux, vérifiez que la version du noyau Linux correspond à la version 2.6.35 ou à une version ultérieure.
- Vérifiez que la machine virtuelle est sous tension.
- Privilège requis (Relais d'hôte ESXi) : **Machine virtuelle.Configuration.Ajouter ou supprimer un périphérique**

#### Procédure

- 1 Cliquez avec le bouton droit de la souris sur une machine virtuelle dans l'inventaire vSphere et sélectionnez **Modifier les paramètres**.
- 2 Dans l'onglet **Matériel virtuel**, cliquez sur **Ajouter un périphérique** et dans le menu déroulant sélectionnez **Contrôleur USB**.

Le contrôleur s'affiche dans la liste des périphériques **Matériel virtuel**.

- 3 Pour modifier le type de contrôleur USB, développez **Nouveau contrôleur USB**.

Si des erreurs de compatibilité s'affichent, vous devez les corriger avant de pouvoir ajouter le contrôleur.

- 4 Cliquez sur **OK**.

#### Étape suivante

Ajoutez un ou plusieurs périphériques USB à la machine virtuelle.

## Ajouter des contrôleurs SCSI dans VMware Host Client

Vous pouvez ajouter des contrôleurs SCSI à une machine virtuelle existante en ajoutant des disques durs sur des numéros inutilisés de bus SCSI.

L'ajout d'un nouveau disque dur sur un numéro inutilisé de bus SCSI crée un nouveau contrôleur SCSI.

#### Conditions préalables

Mettez la machine virtuelle hors tension.

#### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez avec le bouton droit sur une machine virtuelle de la liste et sélectionnez **Modifier les paramètres** dans le menu contextuel.
- 3 Sur l'onglet **Matériel virtuel**, sélectionnez **Ajouter un disque dur** et sélectionnez **Nouveau disque dur** dans le menu déroulant.
- 4 Développez le disque dur pour afficher toutes les options.

- 5 Dans la section **Emplacement du contrôleur**, sélectionnez un numéro de bus SCSI non utilisé dans le menu déroulant.

Par exemple, les numéros de bus et de périphérique 0:0 - 0:15 sont employés par le contrôleur SCSI initial. Le deuxième contrôleur SCSI emploie les numéros de bus et de périphérique 1:0 - 1:15.

- 6 Cliquez sur **Enregistrer**.

#### Résultats

Le nouveau disque dur et le nouveau contrôleur de SCSI sont créés en même temps.

## Changer la configuration du partage de bus SCSI dans VMware Host Client

Vous pouvez définir le type de partage de bus SCSI pour une machine virtuelle et indiquer si le bus SCSI doit être partagé. Selon le type de partage, les machines virtuelles peuvent accéder en même temps au même disque virtuel sur le même serveur ou sur n'importe quel serveur.

Vous pouvez changer la configuration du contrôleur SCSI d'une machine virtuelle uniquement si la machine virtuelle se trouve sur un hôte ESXi.

#### Conditions préalables

Mettez la machine virtuelle hors tension.

#### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez avec le bouton droit sur une machine virtuelle de la liste et sélectionnez **Modifier les paramètres** dans le menu contextuel.
- 3 Sur l'onglet **Matériel virtuel**, développez le contrôleur SCSI que vous souhaitez modifier.
- 4 Sélectionnez le type de partage dans la liste **Partage de bus de SCSI**.

| Option          | Description  |
|-----------------|--|
| <b>Aucun</b>    | Les disques virtuels ne peuvent pas être partagés par d'autres machines virtuelles.                |
| <b>Virtuel</b>  | Les disques virtuels peuvent être partagés par des machines virtuelles sur le même serveur.        |
| <b>Physique</b> | Les disques virtuels peuvent être partagés par les machines virtuelles sur n'importe quel serveur. |

- 5 Cliquez sur **Enregistrer**.

## Changer le type de contrôleur SCSI dans VMware Host Client

Vous pouvez attacher des disques virtuels et des RDM aux machines virtuelles en configurant un contrôleur SCSI virtuel sur les machines virtuelles.

Le choix du contrôleur SCSI n'affecte pas le type IDE ou SCSI de votre disque virtuel. L'adaptateur IDE est toujours de type ATAPI. La valeur par défaut de votre système d'exploitation client est déjà sélectionnée. Les systèmes d'exploitation invités plus anciens disposent d'un adaptateur BusLogic comme contrôleur par défaut.

Si vous créez une machine virtuelle de logique de LSI et ajoutez un disque virtuel qui utilise des adaptateurs de BusLogic, la machine virtuelle démarre à partir du disque d'adaptateurs de BusLogic. LSI Logic SAS est disponible uniquement pour les machines virtuelles avec la version matérielle 7 ou une version suivante. Les disques avec des snapshots ne peuvent pas gagner en performances lorsqu'ils sont utilisés sur des adaptateurs LSI Logic SAS, VMware et LSI Logic Parallel .

---

**Attention** Le changement de type de contrôleur de SCSI peut avoir comme conséquence un échec du démarrage de la machine virtuelle.

---

#### Conditions préalables

Mettez la machine virtuelle hors tension.

#### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez avec le bouton droit sur une machine virtuelle de la liste et sélectionnez **Modifier les paramètres** dans le menu contextuel.
- 3 Cliquez sur l'onglet **Matériel virtuel** et développez un contrôleur SCSI.
- 4 Sélectionnez un type de contrôleur SCSI dans le menu déroulant.
- 5 Cliquez sur **Enregistrer**.

## À propos des contrôleurs SCSI paravirtuels VMware

Les contrôleurs paravirtuels SCSI de VMware sont des contrôleurs de stockage hautes performances qui peuvent augmenter le débit et réduire l'utilisation du CPU. Ces contrôleurs sont mieux adaptés aux environnements de stockage hautes performances.

Les contrôleurs SCSI paravirtuels VMware sont disponibles pour les machines virtuelles avec une compatibilité ESXi 4.x et versions ultérieures. Les disques sur ces contrôleurs peuvent ne pas présenter des gains de performances optimaux s'ils ont des snapshots ou si la mémoire sur l'hôte ESXi est surdédiée. Ce comportement ne saurait atténuer le gain de performance global de l'utilisation des contrôleurs SCSI paravirtuel VMware par rapport aux autres options de contrôleur SCSI.

Pour la prise en charge de la plate-forme des contrôleurs VMware Paravirtual SCSI, reportez-vous au *Guide de compatibilité de VMware* à l'adresse <http://www.vmware.com/resources/compatibility>.



## Ajouter un contrôleur Paravirtual SCSI dans VMware Host Client

Vous pouvez ajouter un contrôleur de stockage haute performance SCSI paravirtuel de VMware pour obtenir un plus grand débit et une plus faible utilisation de CPU.

Les contrôleurs VMware Paravirtual SCSI sont mieux adaptés aux environnements, notamment SAN, qui exécutent des applications à forte activité E/S.

### Conditions préalables

- Vérifiez que la machine virtuelle dispose d'un système d'exploitation invité avec VMware Tools installé.
- Vérifiez que la machine virtuelle utilise la version matérielle 7 ou une version ultérieure.
- Familiarisez-vous avec les limitations des contrôleurs VMware Paravirtual SCSI. Reportez-vous à la section *Administration d'une machine virtuelle vSphere*.
- Pour accéder aux périphériques de disque de démarrage attachés à un contrôleur VMware Paravirtual SCSI, vérifiez que la machine virtuelle dispose d'un système d'exploitation invité Windows 2003 ou Windows 2008.
- Dans certains systèmes d'exploitation, avant de changer le type de contrôleur, vous devez créer une machine virtuelle avec un contrôleur LSI Logic et installer VMware Tools.

Mettez la machine virtuelle hors tension.

### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez avec le bouton droit sur une machine virtuelle de la liste et sélectionnez **Modifier les paramètres** dans le menu contextuel.
- 3 Sur l'onglet **Matériel virtuel**, cliquez sur **Ajouter un autre périphérique** et sélectionnez **Contrôleur SCSI** dans le menu déroulant.  
Les nouveaux contrôleurs SCSI figurent dans la liste du matériel.
- 4 Cliquez sur **Nouveau contrôleur SCSI** et sélectionnez **VMware Paravirtual** dans le menu déroulant.
- 5 Cliquez sur **Enregistrer**.

## Ajouter un contrôleur SATA à une machine virtuelle dans VMware Host Client

Si une machine virtuelle possède plusieurs disques durs ou périphériques CD/DVD-ROM, vous pouvez ajouter jusqu'à trois contrôleurs SATA supplémentaires auxquels affecter les périphériques. Lorsque vous attribuez les périphériques à différents contrôleurs, vous pouvez améliorer les performances et éviter la congestion du trafic de données. Vous pouvez également ajouter des contrôleurs si vous devez dépasser la limite de 30 périphériques pour un seul contrôleur.

Vous pouvez démarrer des machines virtuelles à partir des contrôleurs SATA et les utiliser pour des disques durs virtuels de grande capacité.

Tous les systèmes d'exploitation invités ne prennent pas en charge les contrôleurs SATA AHCI. En général, lorsque vous créez des machines virtuelles avec ESXi 5.5 (et les versions ultérieures) et des systèmes d'exploitation invités Mac OS X, un contrôleur SATA est ajouté par défaut au disque dur virtuel et aux périphériques CD/DVD-ROM. La plupart des systèmes d'exploitation invités, y compris Windows Vista et les versions ultérieures, disposent d'un contrôleur SATA par défaut pour les périphériques CD/DVD-ROM. À des fins de vérification, reportez-vous au *Guide de compatibilité de VMware* approprié à l'adresse <http://www.vmware.com/resources/compatibility>.

#### Conditions préalables

- Vérifiez que la machine virtuelle est compatible avec ESXi 5.5 et versions ultérieures.
- Vérifiez que vous connaissez bien le comportement et les limitations des contrôleurs de stockage. Voir *Administration d'une machine virtuelle vSphere*.
- Vérifiez que vous disposez du privilège **Machine virtuelle.Configuration.Ajouter ou supprimer périphérique** sur la machine virtuelle.
- Mettez la machine virtuelle hors tension.

#### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez avec le bouton droit sur une machine virtuelle de la liste et sélectionnez **Modifier les paramètres** dans le menu contextuel.
- 3 Sur l'onglet **Matériel virtuel**, sélectionnez **Ajouter un autre périphérique** et sélectionnez **Contrôleur SATA** dans le menu déroulant.

Le contrôleur SATA apparaît dans la liste du matériel.

- 4 Cliquez sur **Enregistrer**.

## Ajouter un contrôleur NVMe dans VMware Host Client

Si une machine virtuelle possède plusieurs disques durs, vous pouvez ajouter jusqu'à quatre contrôleurs NVMe virtuels auxquels attribuer les disques. L'utilisation d'un contrôleur NVMe réduit considérablement la surcharge logicielle pour le traitement d'E/S de SE invité, par rapport aux contrôleurs SCSI ou SATA AHCI.

Les contrôleurs NVMe sont plus efficaces avec des disques virtuels sur une baie de disques intégralement Flash, un SSD NVMe local et un stockage PMem.

#### Conditions préalables

- Vérifiez que la machine virtuelle est dotée d'un système d'exploitation invité prenant en charge NVMe.
- Vérifiez que la machine virtuelle est compatible avec ESXi 6.5 ou version ultérieure.

- Vérifiez que vous connaissez bien le comportement et les limitations des contrôleurs de stockage. Pour plus d'informations, consultez le guide d'*Administration d'une machine virtuelle*.
- Vérifiez que vous disposez du privilège **Machine virtuelle.Configurer.Ajouter un nouveau disque** sur la machine virtuelle.

#### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez avec le bouton droit sur une machine virtuelle de la liste et sélectionnez **Modifier les paramètres** dans le menu contextuel.
- 3 Sous l'onglet **Matériel virtuel**, cliquez sur **Ajouter un autre périphérique** et sélectionnez **Contrôleur NVMe** dans le menu déroulant.

#### Résultats

Un nouveau contrôleur NVMe est ajouté à la machine virtuelle.

#### Étape suivante

Vous pouvez ajouter un disque dur à la machine virtuelle et l'attribuer au contrôleur NVMe.

## Autre configuration de périphérique de machine virtuelle dans VMware Host Client

En plus de configurer le CPU et la mémoire de la machine virtuelle et d'ajouter des disques durs et des cartes réseau virtuelles, vous pouvez également ajouter et configurer du matériel virtuel tel que des lecteurs de DVD/CD-ROM, des lecteurs de disquettes et des périphériques SCSI. Vous pouvez également ajouter un temporisateur de surveillance virtuel (VWDT), un périphérique d'horloge de précision et des périphériques PCI.

## Ajouter un lecteur de CD-ROM ou de DVD-ROM à une machine virtuelle dans VMware Host Client

Vous pouvez utiliser un lecteur physique sur un client ou un hôte ou une image ISO pour ajouter un lecteur de CD/DVD à une machine virtuelle.

Si vous voulez ajouter un lecteur CD/DVD qui est sauvegardé par un lecteur CD/DVD USB sur l'ordinateur hôte, vous devez ajouter le lecteur comme un périphérique SCSI. L'ajout ou la suppression à chaud de périphériques SCSI depuis un hôte ESXi n'est pas pris(e) en charge.

#### Conditions préalables

Mettez la machine virtuelle hors tension.

#### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.

- 2 Cliquez avec le bouton droit sur une machine virtuelle de la liste et sélectionnez **Modifier les paramètres** dans le menu contextuel.
- 3 Sur l'onglet **Matériel virtuel**, sélectionnez **Ajouter un autre périphérique** et sélectionnez **Lecteur de CD/DVD** dans le menu déroulant.
- 4 Développez **Lecteur de CD/DVD** et sélectionnez une option.

| Option                       | Description  |
|------------------------------|--|
| Utiliser le lecteur physique | <ol style="list-style-type: none"> <li>a Sélectionnez <b>Périphérique client</b> comme emplacement.</li> <li>b Dans le menu déroulant <b>Mode du périphérique</b>, sélectionnez <b>Émuler le CD-ROM</b> ou <b>Utiliser le relais sur le CD-ROM</b>.</li> </ol>           |
| Utiliser l'image ISO         | <ol style="list-style-type: none"> <li>a Sélectionnez <b>Fichier ISO de la banque de données</b> comme emplacement.</li> <li>b Tapez le chemin d'accès et le nom de fichier pour le fichier image ou cliquez sur <b>Parcourir</b> pour rechercher le fichier.</li> </ol> |

- 5 Si vous ne voulez pas que le lecteur de CD-ROM se connecte quand la machine virtuelle démarre, désélectionnez **Connexion à la mise sous tension**.
- 6 Sélectionnez le nœud de périphérique virtuel que le lecteur emploie dans la machine virtuelle.
- 7 Cliquez sur **Enregistrer**.

## Ajouter un lecteur de disquette à une machine virtuelle dans VMware Host Client

Employez un lecteur de disquettes physique ou une image disquette pour ajouter un lecteur de disquettes à une machine virtuelle.

ESXi ne prend pas en charge les lecteurs de disquettes sauvegardés par un lecteur de disquettes physique sur l'hôte.

### Conditions préalables

- Mettez la machine virtuelle hors tension.
- Vérifiez que vous disposez du privilège **Machine virtuelle.Configuration.Ajouter ou supprimer périphérique** sur la machine virtuelle.

### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez avec le bouton droit sur une machine virtuelle de la liste et sélectionnez **Modifier les paramètres** dans le menu contextuel.
- 3 Sur l'onglet **Matériel virtuel**, sélectionnez **Ajouter un autre périphérique** et sélectionnez **Lecteur de disquettes** dans le menu déroulant.

Le lecteur de disquettes apparaît dans la liste du matériel.

- 4 Développez **Lecteur de disquettes** et sélectionnez le type de périphérique à utiliser.

| Option   | Description  |
|--|--|
| <b>Périphérique Client</b>                       | Sélectionnez cette option pour connecter le lecteur de disquettes à un lecteur de disquettes physique ou à une image de disquette .flp sur le système à partir duquel vous accédez à VMware Host Client .  |
| <b>Utiliser une image de disquette existante</b> | <p>a Sélectionnez cette option pour connecter le périphérique virtuel à une image existante d'un lecteur de disquettes sur une banque de données accessible à l'hôte.</p> <p>b Cliquez sur <b>Parcourir</b> et sélectionnez l'image disquette.</p> |

- 5 (Facultatif) Sélectionnez **Connexion à la mise sous tension** pour configurer le périphérique de manière à ce qu'il se connecte lors de la mise sous tension de la machine virtuelle.
- 6 Cliquez sur **Enregistrer**.

## Ajouter un périphérique USB à une machine virtuelle dans VMware Host Client

À l'aide de VMware Host Client, vous pouvez ajouter un périphérique USB à une machine virtuelle.

### Conditions préalables

- Vérifiez qu'un contrôleur USB est présent. Reportez-vous à la section [Ajouter un contrôleur USB à une machine virtuelle](#).
- Ajoutez un périphérique USB physique à l'hôte ESXi où se trouve la machine virtuelle en le connectant à l'hôte.

**Note** Si l'hôte ESXi ne dispose pas de périphériques USB, vous ne pouvez pas ajouter de périphérique USB à la machine virtuelle.

### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez avec le bouton droit sur la machine virtuelle dans la liste et sélectionnez **Modifier les paramètres** dans le menu contextuel.
- 3 Dans l'onglet **Matériel virtuel**, sélectionnez **Ajouter un autre périphérique**, puis **Périphérique USB** dans le menu déroulant.  
  
Le périphérique USB figure dans la liste des périphériques matériels dont dispose la machine virtuelle.
- 4 Dans la liste déroulante **Périphérique USB**, sélectionnez le périphérique USB à ajouter à la machine virtuelle.
- 5 Cliquez sur **Enregistrer**.

## Ajouter un contrôleur audio à une machine virtuelle dans VMware Host Client

À l'aide de VMware Host Client, vous pouvez ajouter un contrôleur audio à une machine virtuelle.

### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez avec le bouton droit sur une machine virtuelle de la liste et sélectionnez **Modifier les paramètres** dans le menu contextuel.
- 3 Dans l'onglet **Matériel virtuel**, sélectionnez **Ajouter un autre périphérique**, puis **Contrôleur audio** dans le menu déroulant.

Le contrôleur audio apparaît dans la liste des périphériques matériels disponibles pour la machine virtuelle.

- 4 Dans le menu déroulant **Adaptateur son**, sélectionnez le contrôleur audio à connecter à la machine virtuelle.
- 5 Cliquez sur **Enregistrer**.

## Configuration de ports parallèles et de ports série dans VMware Host Client

Les ports série et parallèle sont des interfaces permettant de connecter des périphériques à la machine virtuelle. Le port série virtuel peut se connecter à un port série physique ou à un fichier sur l'ordinateur hôte. Vous pouvez aussi l'utiliser pour établir une connexion directe entre deux machines virtuelles ou entre une machine virtuelle et une application sur l'ordinateur hôte. Vous pouvez ajouter des ports parallèles et série et changer la configuration des ports série.

### Ajouter un port série à une machine virtuelle dans VMware Host Client

Une machine virtuelle peut employer jusqu'à quatre ports série virtuels. Vous pouvez connecter le port série virtuel à un port série physique ou à un fichier sur l'ordinateur hôte. Vous pouvez également utiliser un canal nommé côté hôte pour configurer une connexion directe entre deux machines virtuelles ou entre une machine virtuelle et une application sur l'ordinateur hôte. En outre, vous pouvez utiliser un port ou un URI vSPC (Virtual Serial Port Concentrator) pour connecter un port série sur le réseau.

### Conditions préalables

- Familiarisez-vous avec les différents types de supports auxquels le port peut accéder, les connexions vSPC et les conditions qui peuvent s'appliquer. Voir *Administration d'une machine virtuelle vSphere*.
- Pour connecter un port série sur un réseau, ajoutez un ensemble de règles de pare-feu. Voir *Administration d'une machine virtuelle vSphere*.
- Privilège nécessaire : **Machine virtuelle .Configuration.Ajouter ou supprimer un périphérique**

Mettez la machine virtuelle hors tension.

#### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez avec le bouton droit sur une machine virtuelle de la liste et sélectionnez **Modifier les paramètres** dans le menu contextuel.
- 3 Sur l'onglet **Matériel virtuel**, sélectionnez **Ajouter un autre périphérique** et sélectionnez **Port série**.

Le port série apparaît dans la liste du matériel.

- 4 Dans la liste du matériel, développez le port série et sélectionnez le type de port multimédias auquel accéder.

| Option                          | Description   |
|---------------------------------|---|
| Utiliser un fichier de sortie   | Naviguez jusqu'à l'emplacement du fichier sur l'hôte pour stocker le résultat du port série virtuel.  |
| Utiliser un port série physique | Sélectionnez le port dans le menu déroulant.  |
| Utiliser le canal nommé         | <ol style="list-style-type: none"> <li>Entrez un nom pour le canal dans le champ de <b>Nom de canal</b>.</li> <li>Sélectionnez les valeurs <b>Extrémité proche</b> et <b>Extrémité lointaine</b> pour le canal dans les menus déroulants.</li> </ol>  |
| Utiliser le réseau              | <ol style="list-style-type: none"> <li>Dans le menu déroulant, sélectionnez <b>Direction</b>, sélectionnez <b>Serveur</b> ou <b>Client</b>.</li> <li>Saisissez l'URI du port.<br/><br/>L'URI est l'extrémité distante du port série auquel le port série de la machine virtuelle devrait se connecter.</li> <li>Si vous utilisez vSPC comme étape intermédiaire pour accéder à toutes les machines virtuelles via une seule adresse IP, sélectionnez <b>Utiliser le concentrateur virtuel de port série</b> et entrez l'emplacement de l'URI vSPC.</li> </ol> |

- 5 (Facultatif) Désélectionnez **Connexion à la mise sous tension** si vous ne voulez pas que le périphérique du port parallèle se connecte lorsque la machine virtuelle est mise sous tension.
- 6 Cliquez sur **Enregistrer**.

#### Exemple : Établissement de connexions réseau à un client ou un serveur via un port série sans paramètres d'authentification

Si vous n'utilisez pas vSPC et configurez la machine virtuelle avec un port série connecté comme serveur avec l'URI `telnet://:12345`, vous pouvez vous connecter au port série de la machine virtuelle depuis le système d'exploitation Linux ou Windows.

```
telnet yourESXiServerIPAddress 12345
```

De même, si vous exécutez le serveur Telnet sur le port 23 du système Linux (`telnet://yourLinuxBox:23`), configurez la machine virtuelle comme URI de client.

```
telnet://yourLinuxBox:23
```

La machine virtuelle établit une connexion sur le port 23 du système Linux.

## Ajouter un port parallèle à une machine virtuelle dans VMware Host Client

Pour connecter des périphériques à des machines virtuelles, telles que des imprimantes et des scanners, vous pouvez utiliser un port parallèle. Vous envoyez la sortie de ces dispositifs dans un fichier sur l'ordinateur hôte.

**Note** Pour ajouter un port parallèle à une machine virtuelle qui s'exécute sur un hôte ESXi 4.1 ou une version antérieure d'hôte, vous pouvez également choisir d'envoyer la sortie à un port parallèle physique sur l'hôte. Cette option n'est pas disponible avec un hôte ESXi 5.0 et versions ultérieures.

### Conditions préalables

- Mettez la machine virtuelle hors tension.
- Vérifiez que vous disposez du privilège **Machine virtuelle.Configuration.Ajouter ou supprimer périphérique** sur la machine virtuelle.

### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez avec le bouton droit sur une machine virtuelle de la liste et sélectionnez **Modifier les paramètres** dans le menu contextuel.
- 3 Sur l'onglet **Matériel virtuel**, sélectionnez **Ajouter un autre périphérique** et sélectionnez **Port parallèle**.

Le port parallèle apparaît dans la liste du matériel.

- 4 Développez le port parallèle et dans le champ Connexion, accédez à un dossier où créer le fichier.

Le chemin du fichier apparaît dans la zone de texte **Connexion**.

- 5 (Facultatif) Sélectionnez **Connexion à la mise sous tension** pour configurer le périphérique de manière à ce qu'il se connecte lors de la mise sous tension de la machine virtuelle.
- 6 Cliquez sur **Enregistrer**.

## Utilisation d'un temporisateur de surveillance virtuel

Pour garantir une auto-dépendance liée aux performances du système dans une machine virtuelle, vous pouvez ajouter un temporisateur de surveillance virtuel (VWDT). Si le système d'exploitation invité cesse de répondre et ne parvient pas à récupérer tout seul à cause de



problèmes logiciels ou d'erreurs, le temporisateur de surveillance virtuel attend une période prédéfinie, puis redémarre le système.

Vous pouvez activer le temporisateur de surveillance virtuel pour qu'il démarre soit par le système d'exploitation invité soit par le BIOS ou le microprogramme EFI. Si vous avez choisi de démarrer le temporisateur de surveillance virtuel par le BIOS ou le microprogramme EFI, il démarre avant le démarrage du système d'exploitation invité.

Le temporisateur de surveillance virtuel joue un rôle important dans les solutions de clustering basées sur l'invité où chaque machine virtuelle dans le cluster peut récupérer tout seul en cas d'échec.

## Ajouter un temporisateur de surveillance virtuel à une machine virtuelle dans VMware Host Client

Vous pouvez ajouter un temporisateur de surveillance virtuel à une machine virtuelle pour la protéger d'une panne du système d'exploitation invité pendant une période prolongée.

### Conditions préalables

- Mettez la machine virtuelle hors tension.
- Vérifiez que vous disposez du privilège **Machine virtuelle.Configuration.Ajouter ou supprimer périphérique** sur la machine virtuelle.
- Vérifiez que le système d'exploitation invité de la machine virtuelle prend en charge le périphérique VVDT.
- Vérifiez que la version du matériel virtuel est la version 17.

### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez avec le bouton droit sur une machine virtuelle de la liste et sélectionnez **Modifier les paramètres** dans le menu contextuel.
- 3 Dans l'onglet **Matériel virtuel**, sélectionnez **Ajouter un autre périphérique**, puis cliquez sur **Temporisateur de surveillance**.

Le temporisateur de surveillance figure dans la liste de matériel.

- 4 (Facultatif) Sélectionnez **Démarrer avec le démarrage BIOS/EFI** pour démarrer le temporisateur de surveillance par le microprogramme BIOS ou EFI.

Lorsque vous sélectionnez cette option, le périphérique VVDT démarre avant le système d'exploitation invité. Si le démarrage du système d'exploitation invité prend trop de temps ou ne prend pas en charge le temporisateur de surveillance, il se peut que le périphérique redémarre constamment la machine virtuelle.

- 5 Cliquez sur **Enregistrer**.

## Ajouter un périphérique horloge de précision à une machine virtuelle dans VMware Host Client

Une horloge de précision est un périphérique virtuel qui s'exécute sur une machine virtuelle et qui accède à l'heure du système d'un hôte. L'ajout d'une horloge de précision à une machine virtuelle garantit la synchronisation de l'heure et l'horodatage de haute précision.

### Conditions préalables

- Mettez la machine virtuelle hors tension.
- Vérifiez que la version du matériel virtuel est la version 17.
- Vérifiez que vous disposez du privilège **Machine virtuelle.Configuration.Ajouter ou supprimer périphérique** sur la machine virtuelle.
- Vérifiez que vous disposez du privilège **Machine virtuelle.Configuration.Modifier les paramètres de périphérique** sur la machine virtuelle.

### Procédure

- 1 Dans l'inventaire de VMware Host Client, cliquez sur **Machines virtuelles**.
- 2 Cliquez avec le bouton droit sur une machine virtuelle de la liste et sélectionnez **Modifier les paramètres** dans le menu contextuel.
- 3 Dans l'onglet **Matériel virtuel**, cliquez sur **Ajouter un autre périphérique** et sélectionnez **Horloge de précision**.

Le périphérique horloge de précision apparaît dans la liste du matériel.

- 4 (Facultatif) Sélectionnez le protocole de synchronisation de l'heure.
- 5 Cliquez sur **Enregistrer**.

## Ajouter un périphérique PCI à une machine virtuelle dans VMware Host Client

L'E/S DirectPath permet au système d'exploitation invité d'une machine virtuelle d'accéder directement aux périphériques PCI et PCIe physiques connectés à un hôte. En utilisant cette technologie, vous pouvez connecter chaque machine virtuelle à un maximum de seize périphériques PCI physiques. Vous pouvez utiliser Dynamic DirectPath I/O pour attribuer plusieurs périphériques de relais PCI à une machine virtuelle. À partir de vSphere 7.0, vous pouvez identifier les périphériques de relais PCI par leurs noms de fournisseur et de modèle.

---

**Note** Certaines opérations de machine virtuelle ne sont plus disponibles lorsque vous ajoutez un périphérique de relais PCI ou PCIe à la machine virtuelle.

---

Pour plus d'informations sur la configuration d'étiquette de matériel, reportez-vous à la section [Changer l'étiquette de matériel dans VMware Host Client](#).

### Conditions préalables

- Mettez la machine virtuelle hors tension.
- Vérifiez que vous disposez du privilège **Machine virtuelle.Configuration.Ajouter ou supprimer périphérique** sur la machine virtuelle.
- Vérifiez que les périphériques PCI sont connectés à l'hôte et qu'ils sont disponibles pour la fonction de relais.
- Si vous souhaitez ajouter un périphérique PCI dynamique à une machine virtuelle, vérifiez que la version du matériel virtuel est la 17.

### Procédure

- 1 Dans l'inventaire de VMware Host Client, cliquez sur **Machines virtuelles**.
- 2 Cliquez avec le bouton droit sur une machine virtuelle de la liste et sélectionnez **Modifier les paramètres** dans le menu contextuel.
- 3 Dans l'onglet **Matériel virtuel**, cliquez sur **Ajouter un autre périphérique** et sélectionnez un périphérique.

| Option                     | Action   |
|----------------------------|--|
| périphérique PCI           | <ol style="list-style-type: none"> <li>a Cliquez sur <b>Périphérique PCI</b>.<br/>Un nouveau périphérique apparaît dans la liste du matériel.</li> <li>b Dans le menu déroulant, sélectionnez un périphérique PCI pour vous connecter à la machine virtuelle.</li> </ol>   |
| Périphérique PCI dynamique | <ol style="list-style-type: none"> <li>a Cliquez sur <b>Périphérique PCI dynamique</b>.<br/>Un nouveau périphérique apparaît dans la liste du matériel.</li> <li>b Développez <b>Nouveau périphérique PCI</b>, puis dans le menu déroulant, sélectionnez les périphériques de relais PCI à connecter à la machine virtuelle.<br/><br/>Vous pouvez identifier les périphériques de relais PCI en fonction du fournisseur, du nom de modèle et de l'étiquette de matériel. Les étiquettes de matériel, le cas échéant, sont affichées entre crochets.</li> </ol> <p><b>Note</b> Lorsque vous ajoutez un périphérique PCI à une machine virtuelle, la taille de la mémoire totale de la machine virtuelle est automatiquement réservée.</p> |

- 4 Cliquez sur **Enregistrer**.

## Sécurisation des machines virtuelles dans VMware Host Client

Le système d'exploitation invité exécuté dans la machine virtuelle est exposé aux mêmes risques de sécurité qu'une machine physique. Pour optimiser la sécurité de votre environnement virtuel, vous pouvez ajouter un vTPM (Virtual Trusted Platform Module) à vos hôtes ESXi. Vous pouvez également activer la sécurité basée sur la virtualisation (VBS) pour les machines virtuelles qui

exécutent les systèmes d'exploitation Windows 10 et Windows Server 2016 les plus récents. Vous pouvez fournir une sécurité supplémentaire à vos charges de travail à l'aide de vSGX (Virtual Intel® Software Guard Extensions) pour les machines virtuelles.

## Activer vSGX sur une machine virtuelle dans VMware Host Client

Pour protéger le contenu des enclaves contre la divulgation et les modifications, vous pouvez activer vSGX sur une machine virtuelle dans VMware Host Client.

### Sécuriser les machines virtuelles avec vSGX

vSphere vous permet de configurer vSGX pour les machines virtuelles. Certains processeurs Intel modernes mettent en œuvre une extension de sécurité appelée Intel® Software Guard Extension (Intel® SGX). Intel SGX permet de définir des régions privées de mémoire, appelées enclaves, pour le code au niveau utilisateur. Intel SGX protège le contenu des enclaves contre la divulgation ou la modification de telle sorte que le code exécuté en dehors de l'enclave ne puisse pas y accéder.

vSGX permet aux machines virtuelles d'utiliser la technologie Intel SGX si elle est disponible sur le matériel. Pour utiliser vSGX l'hôte ESXi doit être installé sur un CPU compatible SGX et SGX doit être activé dans le BIOS de l'hôte ESXi. Vous pouvez utiliser vSphere Client pour activer SGX pour une machine virtuelle. Pour plus d'informations, consultez la documentation *Sécurité vSphere*.

Certaines opérations et fonctionnalités ne sont pas compatibles avec SGX.

- Migration avec Storage vMotion
- Interruption ou reprise de la machine virtuelle
- Prise d'un snapshot de la machine virtuelle
- Fault Tolerance
- Activation de l'intégrité de l'invité (GI, fondation de plateforme pour VMware AppDefense 1.0)

### Conditions préalables

- Mettez la machine virtuelle hors tension.
- Vérifiez que la machine virtuelle utilise le microprogramme EFI.
- Vérifiez que l'hôte ESXi est de version 7.0 ou ultérieure.
- Vérifiez que le système d'exploitation invité de la machine virtuelle est Linux, Windows 10 (64 bits) ou versions ultérieures, ou Windows Server 2016 (64 bits) ou versions ultérieures.
- Vérifiez que vous disposez du privilège **Machine virtuelle.Configuration.Modifier les paramètres de périphérique** sur la machine virtuelle.
- Vérifiez que l'hôte ESXi est installé sur un CPU compatible SGX et que SGX est activé dans le BIOS de l'hôte ESXi. Pour plus d'informations sur les CPU pris en charge, consultez l'article à l'adresse <https://kb.vmware.com/s/article/71367>.

**Procédure**

- 1 Dans l'inventaire de VMware Host Client, cliquez sur **Machines virtuelles**.
- 2 Cliquez avec le bouton droit sur une machine virtuelle de la liste et sélectionnez **Modifier les paramètres** dans le menu contextuel.
- 3 Dans l'onglet **Matériel virtuel**, développez **Périphériques de sécurité**.
- 4 Cochez la case **Activer**.
- 5 Sous **Taille du cache de la page d'enclave**, entrez une nouvelle valeur dans la zone de texte et sélectionnez la taille en Mo ou Go dans le menu déroulant.

**Note** La taille du cache de la page enclave doit être un multiple de 2.

- 6 Dans le menu déroulant **Lancer la configuration du contrôle**, sélectionnez le mode approprié.

| Option       | Action   |
|--------------|--|
| Verrouillé   | Active la configuration de l'enclave de lancement.<br>Sous <b>Lancer le hachage de la clé publique d'enclave</b> , entrez un hachage SHA256 valide.<br>La clé de hachage SHA256 doit contenir 64 caractères. |
| Déverrouillé | Active la configuration de l'enclave de lancement du système d'exploitation invité.  |

- 7 Cliquez sur **Enregistrer**.

## Désactiver vSGX sur une machine virtuelle dans VMware Host Client

Pour désactiver vSGX sur une machine virtuelle, vous pouvez utiliser VMware Host Client.

**Procédure**

- 1 Dans l'inventaire de VMware Host Client, cliquez sur **Machines virtuelles**.
- 2 Cliquez avec le bouton droit sur une machine virtuelle de la liste et sélectionnez **Modifier les paramètres** dans le menu contextuel.
- 3 Dans l'onglet **Matériel virtuel**, développez **Périphériques de sécurité**.
- 4 Décochez la case **Activer** et cliquez sur **Enregistrer**.

**Résultats**

vSGX est désactivé sur la machine virtuelle.

## Supprimer un périphérique vTPM d'une machine virtuelle dans VMware Host Client

Le TPM (Trusted Platform Module) est une puce spécialisée qui stocke des informations sensibles spécifiques à l'hôte, comme des clés privées et des données secrètes du système d'exploitation. La puce TPM est également utilisée pour effectuer des tâches cryptographiques et attester de

l'intégrité de la plate-forme. Dans VMware Host Client, vous pouvez uniquement supprimer le périphérique vTPM d'une machine virtuelle.

Le périphérique TPM virtuel est une émulation logicielle de la fonctionnalité du TPM. Vous pouvez ajouter un périphérique TPM virtuel (vTPM) pour les machines virtuelles de votre environnement. La mise en œuvre du vTPM ne nécessite pas de puce TPM physique sur l'hôte. ESXi utilise le périphérique vTPM pour exercer la fonctionnalité de TPM dans votre environnement vSphere.

vTPM est disponible pour les machines virtuelles disposant des systèmes d'exploitation Windows 10 et Windows Server 2016. La machine virtuelle doit être de version matérielle 14 ou ultérieure.

Vous pouvez ajouter un périphérique TPM virtuel à une machine virtuelle uniquement dans l'instance vCenter Server. Pour plus d'informations, consultez la documentation *Sécurité vSphere*.

Dans VMware Host Client, vous pouvez uniquement supprimer le périphérique TPM virtuel depuis une machine virtuelle.

#### Conditions préalables

- La machine virtuelle doit être de version matérielle 14 ou ultérieure.
- Le SE invité doit être de version Windows 10 ou Windows Server 2016 et ultérieures.
- La machine virtuelle doit être mise hors tension.

#### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.
- 2 Cliquez avec le bouton droit sur une machine virtuelle de la liste et sélectionnez **Modifier les paramètres** dans le menu contextuel.
- 3 Dans l'onglet **Matériel virtuel**, recherchez le périphérique TPM et cliquez sur l'icône **Supprimer**.

Le périphérique TPM virtuel est supprimé de la machine virtuelle.

- 4 Cliquez sur **Enregistrer** pour fermer l'assistant.

## Activer ou désactiver la sécurité basée sur la virtualisation (VBS) sur une machine virtuelle existante dans VMware Host Client

La sécurité basée sur la virtualisation utilise la technologie de virtualisation basée sur Microsoft Hyper-V pour isoler les services du système d'exploitation Windows de base dans un environnement distinct et virtualisé. Ce type d'isolation offre un niveau de protection supplémentaire, car il rend impossible la manipulation des services clés de votre environnement.

Vous pouvez modifier le niveau de sécurité d'une machine virtuelle en activant ou en désactivant la sécurité basée sur la virtualisation (VBS) Microsoft sur les machines virtuelles existantes pour les systèmes d'exploitation invités Windows pris en charge.

L'activation de la sécurité basée sur la virtualisation sur une machine virtuelle active automatiquement le matériel virtuel dont Windows a besoin pour la fonctionnalité de sécurité basée sur la virtualisation. En activant la sécurité basée sur la virtualisation, une variante d'Hyper-V démarre sur la machine virtuelle et Windows commence à s'exécuter à l'intérieur de la partition racine d'Hyper-V.

La sécurité basée sur la virtualisation est disponible sur les versions les plus récentes du système d'exploitation Windows, par exemple Windows 10 et Windows Server 2016. Pour utiliser la sécurité basée sur la virtualisation sur une machine virtuelle, la machine virtuelle doit être compatible avec ESXi 6.7 et versions ultérieures.

Dans VMware Host Client, vous pouvez activer la sécurité basée sur la virtualisation lors de la création d'une machine virtuelle. Sinon, vous pouvez activer ou désactiver la sécurité basée sur la virtualisation pour une machine virtuelle existante.

### Conditions préalables

La configuration de VBS est un processus qui implique d'abord l'activation de VBS dans la machine virtuelle, puis dans le système d'exploitation invité.

---

**Note** Les nouvelles machines virtuelles configurées pour Windows 10, Windows Serveur 2016 et Windows Server 2019 sur des versions matérielles antérieures à la version 14 sont créées avec le BIOS hérité par défaut. Si vous modifiez le type de microprogramme d'une machine virtuelle à partir du BIOS hérité vers l'interface UEFI, vous devez réinstaller le système d'exploitation invité.

Vous pouvez activer la sécurité basée sur la virtualisation sur une machine virtuelle uniquement si la validation par le TPM de l'hôte est réussie.

---

L'utilisation de CPU Intel pour VBS nécessite vSphere 6.7 ou version ultérieure. La machine virtuelle doit avoir été créée en utilisant la version matérielle 14 ou une version ultérieure et l'un des systèmes d'exploitation invités pris en charge suivants :

- Windows 10 (64 bits) ou versions ultérieures
- Windows Server 2016 (64 bits) ou versions ultérieures

L'utilisation de CPU AMD pour VBS nécessite vSphere 7.0 Update 2 ou version ultérieure. La machine virtuelle doit avoir été créée en utilisant la version matérielle 19 ou une version ultérieure et l'un des systèmes d'exploitation invités pris en charge suivants :

- Windows 10 (64 bits), version 1809 ou versions ultérieures
- Windows Server 2019 (64 bits) ou versions ultérieures

Avant d'activer VBS, assurez-vous d'installer les derniers correctifs pour Windows 10, version 1809 et Windows Server 2019.

### Procédure

- 1 Cliquez sur **Machines virtuelles** dans l'inventaire VMware Host Client.

2 Cliquez avec le bouton droit sur une machine virtuelle de la liste et sélectionnez **Modifier les paramètres** dans le menu contextuel.

3 Dans l'onglet **Options VM**, activez ou désactivez la sécurité basée sur la virtualisation sur la machine virtuelle.

- Pour activer la sécurité basée sur la virtualisation pour la machine virtuelle, cochez la case **Activer la sécurité basée sur la virtualisation**.
- Pour désactiver la sécurité basée sur la virtualisation pour la machine virtuelle, décochez la case **Activer la sécurité basée sur la virtualisation**.

Lorsque vous activez la sécurité basée sur la virtualisation, plusieurs options sont automatiquement sélectionnées et apparaissent en grisé dans l'assistant.

4 Cliquez sur **Enregistrer** pour fermer l'assistant.



# Gestion du stockage dans VMware Host Client

# 6

Lorsque vous vous connectez à un hôte ESXi en utilisant VMware Host Client, vous pouvez effectuer différentes tâches de gestion du stockage sur l'hôte ESXi, y compris la configuration des adaptateurs, la création de banques de données et l'affichage des informations sur les périphériques de stockage.

Ce chapitre contient les rubriques suivantes :

- [Banques de données dans VMware Host Client](#)
- [Gestion des adaptateurs de stockage dans VMware Host Client](#)
- [Gestion des périphériques de stockage dans VMware Host Client](#)
- [Gestion de la mémoire persistante](#)
- [Surveillance du stockage dans VMware Host Client](#)
- [Effectuer une actualisation du stockage et des opérations de réanalyse dans VMware Host Client](#)

## Banques de données dans VMware Host Client

Les banques de données sont des conteneurs logiques, semblables à des systèmes de fichiers, qui contiennent les informations spécifiques de chaque périphérique de stockage et fournissent un modèle uniforme pour stocker des fichiers de machine virtuelle. Vous pouvez également utiliser les banques de données pour stocker des images ISO, des modèles de machine virtuelle, et des images disquette.

Selon le type de stockage utilisé, les banques de données peuvent être des types suivants :

- Système de fichier de la machine virtuelle (VMFS)
- Système de fichier du réseau (NFS)

Vous pouvez augmenter la capacité d'une banque de données après sa création uniquement s'il s'agit d'une banque de données VMFS.

Les périphériques de stockage des blocs ainsi que les périphériques NAS, iSCSI et Fibre Channel prennent en charge l'accélération matérielle.

La fonctionnalité d'accélération matérielle permet à l'hôte ESXi de s'intégrer à des systèmes de stockage conformes. L'hôte peut décharger certaines opérations de gestion de stockage et de machine virtuelle sur les systèmes de stockage. 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 plus d'informations, reportez-vous à l'article de la base de connaissances VMware à l'adresse <http://kb.vmware.com/kb/1021976>.

## Afficher les informations sur les banques de données dans VMware Host Client

Utilisez VMware Host Client pour afficher les banques de données disponibles pour les hôtes et analyser leurs propriétés.

### Procédure

- 1 Cliquez sur **Stockage** dans l'inventaire VMware Host Client et cliquez sur **Banques de données**.
- 2 Pour afficher les détails d'une banque de données spécifique, sélectionnez-la dans la liste.

## Créer une banque de données VMFS dans VMware Host Client

Les banques de données VMFS servent de référentiel aux machines virtuelles. Vous pouvez configurer des banques de données VMFS sur tous les périphériques de stockage basés sur SCSI que votre hôte détecte, y compris Fibre Channel, iSCSI et les périphériques de stockage locaux. Vous pouvez utiliser l'assistant **Nouvelle banque de données** pour créer des banques de données dans VMware Host Client.

### Conditions préalables

Installez et configurez tous les adaptateurs dont votre stockage a besoin. Réanalysez les cartes pour détecter les périphériques de stockage nouvellement ajoutés.

### Procédure

- 1 Cliquez sur **Stockage** dans l'inventaire VMware Host Client et cliquez sur **Banques de données**.
- 2 Cliquez sur **Nouvelle banque de données**.  
L'assistant **Nouvelle banque de données** s'affiche.
- 3 Sur la page Sélectionner un type de création, sélectionnez **Créer une banque de données VMFS** et cliquez sur **Suivant**.

| Option  | Description  |
|---|--|
| <b>Créer une banque de données VMFS</b>                             | Crée une banque de données VMFS sur un périphérique de disque local.   |
| <b>Ajouter une extension à une banque de données VMFS existante</b> | Augmente la taille d'une banque de données existante en ajoutant une nouvelle extension sur un autre disque. |

| Option   | Description  |
|--|--|
| Développer une extension de banque de données VMFS existante | Augmente la taille d'une extension de banque de données existante. |
| Monter une banque de données NFS                             | Crée une banque de données en montant un volume NFS distant.       |

- 4 Sur la page Sélectionner un périphérique, sélectionnez l'emplacement dans lequel créer la nouvelle partition VMFS.
  - a Entrez le nom de la nouvelle banque de données.
  - b Sélectionnez un périphérique auquel ajouter la banque de données.  
La liste contient uniquement les périphériques ayant suffisamment d'espace disponible.
  - c Cliquez sur **Suivant**.
- 5 Sur la page Sélectionner les options de partitionnement, sélectionnez comment partitionner le périphérique et cliquez sur **Suivant**.

| Option                     | Description   |
|----------------------------|---|
| Utiliser le disque complet | Vous indique tout l'espace disponible sur le périphérique.  |
| Personnalisé               | Cliquez sur la barre <b>Espace libre</b> et utilisez le curseur horizontal pour partitionner le périphérique. |

- 6 Sur la page Prêt à terminer, vérifiez les détails de la configuration et cliquez sur **Terminer**.

## Augmentation de la capacité d'une banque de données VMFS

Si votre banque de données VMFS requiert plus d'espace, augmentez la capacité de la banque de données. Vous pouvez augmenter dynamiquement la capacité en agrandissant une extension de la banque de données ou en ajoutant une extension.

Utilisez une des méthodes suivantes pour augmenter la capacité d'une banque de données :

- Agrandissez dynamiquement une extension de banque de données extensible, afin qu'elle remplisse la capacité adjacente disponible. L'extension est considérée comme extensible lorsque le périphérique de stockage sous-jacent dispose d'espace libre immédiatement après l'extension.

- Ajoutez dynamiquement l'extension. La banque de données peut s'étendre sur un maximum de 32 extensions, la taille de chacune d'elles dépassant les 2 To, mais la banque de données s'affichant en tant que volume unique. La banque de données VMFS étendue peut utiliser n'importe laquelle de ses extensions ou toutes ses extensions à tout moment. Elle ne doit pas nécessairement remplir une extension spécifique avant d'utiliser la suivante.

---

**Note** Les banques de données ne prenant en charge que le verrouillage par assistance matérielle, également appelé mécanisme ATS (atomic test and set), ne peuvent s'étendre sur des périphériques non ATS. Pour plus d'informations, consultez [#unique\\_185](#).

---

**Note** Les banques de données ne prenant en charge que le verrouillage par assistance matérielle, également appelé mécanisme ATS (atomic test and set), ne peuvent s'étendre sur des périphériques non ATS. Pour plus d'informations, consultez *Stockage vSphere*.

---

## Augmenter la capacité d'une banque de données VMFS existante dans VMware Host Client

Lorsque vous avez besoin d'ajouter des machines virtuelles à une banque de données ou lorsque les machines virtuelles exécutant sur une banque de données nécessitent plus d'espace, vous pouvez augmenter dynamiquement la capacité d'une banque de données VMFS.

Si une banque de données partagée dispose de machines virtuelles sous tension et qu'elle est complètement remplie, vous pouvez augmenter la capacité de la banque de données uniquement à partir de l'hôte dans lequel les machines virtuelles sous tension sont enregistrées.

### Procédure

- 1 Cliquez sur **Stockage** dans l'inventaire VMware Host Client et cliquez sur **Banques de données**.
- 2 Cliquez sur **Nouvelle banque de données**.
- 3 Sur la page Sélectionner le type de création, cliquez sur **Ajouter une extension à la banque de données VMFS existante** et cliquez sur **Suivant**.
- 4 Sur la page Sélectionnez une banque de données, sélectionnez la banque de données à développer et cliquez sur **Suivant**.
- 5 Sur la page Sélectionner un périphérique, sélectionnez un périphérique sur lequel créer la nouvelle partition VMFS et cliquez sur **Suivant**.
- 6 Sur la page Sélectionner les options de partitionnement, sélectionnez comment partitionner le périphérique et cliquez sur **Suivant**.

| Option                     | Description   |
|----------------------------|---|
| Utiliser le disque complet | Vous indique tout l'espace disponible sur le périphérique.  |
| Personnalisé               | Cliquez sur la barre <b>Espace libre</b> et utilisez le curseur horizontal pour partitionner le périphérique. |

- 7 Sur la page Prêt à terminer, vérifiez les détails de la configuration et cliquez sur **Terminer**.

## Montage d'une banque de données NFS (Network File System) dans VMware Host Client

Avec VMware Host Client, vous pouvez créer une banque de données NFS (Network File System) pour stocker des disques virtuels et pour l'utiliser comme référentiel central pour les images ISO, les machines virtuelles, etc. Un client NFS intégré dans ESXi utilise le protocole NFS (Network File System) sur TCP/IP pour accéder à un volume NFS désigné qui se trouve sur un serveur NAS. vSphere prend en charge les versions 3 et 4.1 du protocole NFS.

L'hôte ESXi peut monter un volume NFS et l'utiliser pour ses besoins de stockage.

En général, le volume ou le répertoire NFS est créé par un administrateur de stockage et exporté depuis le serveur NFS. Vous n'avez pas besoin de formater le volume NFS avec un système de fichiers local tel que VMFS. Vous pouvez plutôt monter le volume directement sur les hôtes ESXi et l'utiliser pour stocker et démarrer les machines virtuelles de la même manière que vous utilisez les banques de données VMFS.

Outre le stockage des disques virtuels sur les banques de données NFS, vous pouvez employer NFS comme référentiel central pour les images ISO, les modèles de machine virtuelle, etc. 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. Vous pouvez ensuite installer un système d'exploitation invité à partir du fichier ISO.

Lorsque vous utilisez un stockage NFS, suivez les directives spécifiques associées à la configuration du serveur NFS, à la mise en réseau, aux banques de données NFS, etc.

### Procédure

#### 1 Monter une banque de données NFS dans VMware Host Client

Utilisez l'assistant **Nouvelle banque de données** pour monter une banque de données NFS (Network File System) dans VMware Host Client.

### Monter une banque de données NFS dans VMware Host Client

Utilisez l'assistant **Nouvelle banque de données** pour monter une banque de données NFS (Network File System) dans VMware Host Client.

#### Conditions préalables

Puisque NFS nécessite une connectivité réseau pour accéder aux données sur les serveurs distants, avant de configurer NFS, vous devez d'abord configurer la mise en réseau VMkernel.

### Procédure

- 1 Cliquez sur **Stockage** dans l'inventaire VMware Host Client et cliquez sur **Banques de données**.
- 2 Cliquez sur **Nouvelle banque de données**.

L'assistant **Nouvelle banque de données** s'affiche.

- 3 Sur la page Sélectionner un type de création, cliquez sur **Monter la banque de données NFS** et cliquez sur **Suivant**.
- 4 Sur la page Fournir les détails du montage NFS, fournissez les renseignements concernant la banque de données NFS que vous montez.
  - a Entrez le nom de la banque de données NFS.
  - b Entrez le nom du serveur NFS.  
 Pour le nom du serveur, vous pouvez entrer une adresse IP, un nom DNS ou un UUID NFS.

---

**Note** 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 sont pas identiques, les hôtes détectent le même volume NFS comme deux banques de données différentes. Il peut s'ensuivre une défaillance de certaines fonctionnalités comme vMotion. Par exemple, ce type de différence se produit si vous nommez le serveur **filer** sur un hôte et **filer.domain.com** sur l'autre.

---

  - c Spécifiez le partage NFS.
  - d Spécifiez la version NFS.
  - e Cliquez sur **Suivant**.
- 5 Sur la page Prêt à terminer, vérifiez les paramètres de configuration de la banque de données NFS et cliquez sur **Terminer**.

## Démonter une banque de données dans VMware Host Client

Lorsque vous démontez une banque de données dans VMware Host Client, elle reste intacte mais vous ne pouvez plus la consulter dans l'inventaire de l'hôte que vous gérez. La banque de données continue d'apparaître sur les autres hôtes, où elle reste montée.

N'exécutez aucune opération de configuration qui puisse générer des E/S vers la banque de données lorsque le démontage est en cours.

### Conditions préalables

---

**Note** Assurez-vous que la banque de données n'est pas utilisée par le signal de pulsation vSphere HA. Le signal de pulsation vSphere HA ne vous empêche pas de démonter la banque de données. Toutefois, si la banque de données est utilisée pour le signal de pulsation, son démontage peut provoquer la défaillance de l'hôte et le redémarrage de toutes les machines virtuelles actives.

---

Avant de démonter une banque de données, veillez à ce que les conditions requises suivantes soient remplies :

- Aucune machine virtuelle ne doit se trouver dans la banque de données
- La fonctionnalité Storage DRS ne gère pas la banque de données.

- Storage I/O Control est désactivé pour cette banque de données.

#### Procédure

- 1 Cliquez sur **Stockage** dans l'inventaire VMware Host Client et cliquez sur **Banques de données**.
- 2 Cliquez avec le bouton droit sur la banque de données à démonter dans la liste et cliquez sur **Démonter**.
- 3 Confirmez que vous voulez démonter la banque de données.

### Échec du démontage ou de la suppression de la banque de données

Lors de votre tentative de démontage ou de suppression d'une banque de données, l'opération échoue.

#### Problème

L'opération de démontage ou de suppression d'une banque de données échoue si la banque de données a des fichiers ouverts. Pour ces opérations utilisateur, l'agent vSphere HA ferme tous les fichiers qu'il a ouverts, par exemple, tous les fichiers à signal de pulsation. Si l'agent est inaccessible par vCenter Server ou si l'agent ne peut pas purger les E/S en attente afin de fermer les fichiers, une défaillance de type L'agent HA de l'hôte '{hostName}' a échoué à mettre au repos l'activité des fichiers de la banque de données '{dsName}' est déclenchée.

#### Cause

Si la banque de données à démonter ou supprimer est utilisée pour le signal de pulsation, vCenter Server l'exclut du signal de pulsation et en choisit une nouvelle. Toutefois, l'agent ne reçoit pas les banques de données à signal de pulsation mises à jour s'il n'est pas accessible, c'est à dire, si l'hôte est isolé ou dans une partition réseau. Dans de tels cas, les fichiers à signal de pulsation ne sont pas fermés et l'opération utilisateur échoue. L'opération peut également échouer si la banque de données est inaccessible suite à des défaillances de stockage telles que l'arrêt de tous les chemins.

---

**Note** Lorsque vous supprimez une banque de données VMFS, cette dernière l'est de tous les hôtes de l'inventaire. Ainsi s'il existe des hôtes dans un cluster vSphere HA qui sont inaccessibles ou qui ne peuvent accéder à la banque de données, l'opération échoue.

---

#### Solution

Assurez-vous que la banque de données est accessible, ainsi que les hôtes concernés.

### Utilisation de l'explorateur de fichiers de banques de données dans VMware Host Client

Utilisez l'explorateur de fichiers de banque de données pour gérer le contenu de votre banque de données. Vous pouvez effectuer plusieurs tâches comme le téléchargement de fichiers dans la

banque de données, le téléchargement des fichiers de la banque de données dans votre système, le déplacement et la copie des dossiers et des fichiers de la banque de données et la création de nouveaux répertoires de banque de données.

## Télécharger des fichiers vers une banque de données dans VMware Host Client

Utilisez l'explorateur de banques de données pour télécharger les fichiers vers les banques de données sur votre hôte.

---

**Note** Virtual Volumes ne prend pas en charge le téléchargement de fichiers directement dans les banques de données virtuelles. Vous devez préalablement créer un dossier dans la banque de données virtuelle, puis télécharger les fichiers dans ce dossier.

---

En plus de leur utilisation classique de stockage de fichiers pour les machines virtuelles, les banques de données peuvent stocker des données ou des fichiers liés aux machines virtuelles. Par exemple, vous pouvez télécharger des images ISO de systèmes d'exploitation depuis un ordinateur local vers une banque de données sur l'hôte. Vous pouvez ensuite utiliser ces images pour installer des systèmes d'exploitation invités sur les nouvelles machines virtuelles.

### Conditions préalables

Privilège nécessaire : **Banque de données.Parcourir la banque de donnée**

### Procédure

- 1 Cliquez sur **Stockage** dans l'inventaire VMware Host Client et cliquez sur **Banques de données**.
- 2 Cliquez sur **Explorateur de banque de données**.
- 3 Sélectionnez la banque de données dans laquelle vous souhaitez stocker le fichier.
- 4 (Facultatif) Cliquez sur **Créer un répertoire** pour créer un répertoire de banque de données où stocker le fichier.
- 5 Sélectionnez le dossier cible et cliquez sur **Télécharger**.
- 6 Localisez l'élément à télécharger depuis votre ordinateur local et cliquez sur **Ouvrir**.  
Le fichier se télécharge dans la banque de données sélectionnée.
- 7 (Facultatif) Actualisez l'explorateur de fichiers de la banque de données pour afficher le fichier téléchargé dans la liste.
- 8 Cliquez sur **Fermer** pour quitter le navigateur.

## Télécharger les fichiers d'une banque de données sur votre système dans VMware Host Client

Utilisez l'explorateur de fichiers des banques de données pour télécharger des fichiers des banques de données disponibles sur l'hôte que vous gérez sur votre système local.



### Conditions préalables

Privilège nécessaire : **Banque de données.Parcourir la banque de donnée**

#### Procédure

- 1 Cliquez sur **Stockage** dans l'inventaire VMware Host Client et cliquez sur **Banques de données**.
- 2 Cliquez sur **Explorateur de banque de données**.
- 3 Sélectionnez la banque de données cible.
- 4 Cliquez sur le dossier qui contient le fichier que vous souhaitez télécharger.  
Les fichiers disponibles dans le dossier sont affichés.
- 5 Cliquez sur le fichier que vous souhaitez télécharger.
- 6 Cliquez sur **Télécharger**.  
Le fichier est téléchargé sur votre système.
- 7 Cliquez sur **Fermer** pour quitter le navigateur.

### Supprimer des fichiers d'une banque de données dans VMware Host Client

Vous pouvez supprimer définitivement des fichiers de n'importe quelle banque de données si vous n'en avez plus besoin.

### Conditions préalables

Privilège nécessaire : **Banque de données.Parcourir la banque de donnée**

#### Procédure

- 1 Cliquez sur **Stockage** dans l'inventaire VMware Host Client et cliquez sur **Banques de données**.
- 2 Cliquez sur **Explorateur de banque de données**.
- 3 Sélectionnez la banque de données cible.
- 4 Sélectionnez le dossier qui contient le fichier que vous souhaitez supprimer.  
Les fichiers disponibles dans le dossier sont affichés.
- 5 Cliquez sur le fichier que vous souhaitez supprimer de la banque de données, cliquez sur **Supprimer** et cliquez de nouveau sur **Supprimer**.
- 6 Cliquez sur **Fermer** pour quitter le navigateur.

## Déplacer des dossiers ou des fichiers de banques de données dans VMware Host Client

Utilisez l'explorateur des fichiers de banque de données pour déplacer des fichiers ou des dossiers vers un nouvel emplacement, sur la même banque de données ou sur une banque de données différente.

---

**Note** Les fichiers de disque virtuel sont déplacés et copiés sans conversion de format. Si vous déplacez un disque virtuel vers une banque de données sur un hôte d'un type différent de l'hôte de source, vous pourriez avoir besoin de convertir les disques virtuels avant de pouvoir les utiliser.

---

### Conditions préalables

Privilège nécessaire : **Banque de données.Parcourir la banque de donnée**

### Procédure

- 1 Cliquez sur **Stockage** dans l'inventaire VMware Host Client et cliquez sur **Banques de données**.
- 2 Cliquez sur **Explorateur de banque de données**.
- 3 Sélectionnez la banque de données cible.
- 4 Sélectionnez le fichier ou le dossier que vous souhaitez déplacer vers un autre emplacement et cliquez sur **Déplacer**.
- 5 Sélectionnez votre destination cible et cliquez sur **Déplacer**.
- 6 Cliquez sur **Fermer** pour quitter le navigateur.

## Copier des dossiers ou des fichiers de banques de données dans VMware Host Client

Utilisez le navigateur de fichiers de banques de données pour copier des dossiers et des fichiers dans un nouvel emplacement, sur la même banque de données ou sur une autre.

---

**Note** Les fichiers de disque virtuel sont déplacés et copiés sans conversion de format. Si vous déplacez un disque virtuel sur une banque de données sur un hôte d'un type différent de l'hôte source, vous pourriez avoir besoin de convertir les disques virtuels.

---

### Conditions préalables

Privilège nécessaire : **Banque de données.Parcourir la banque de donnée**

### Procédure

- 1 Cliquez sur **Stockage** dans l'inventaire VMware Host Client et cliquez sur **Banques de données**.
- 2 Cliquez sur **Explorateur de banque de données**.
- 3 Sélectionnez la banque de données cible.

- 4 Sélectionnez le fichier ou le dossier que vous souhaitez déplacer vers un autre emplacement et cliquez sur **Copier**.
- 5 Sélectionnez votre destination cible et cliquez sur **Copier**.
- 6 Cliquez sur **Fermer** pour quitter le navigateur.

## Créer un nouveau répertoire de banques de données dans VMware Host Client

Vous pouvez créer de nouveaux répertoires de banques de données si vous souhaitez stocker des fichiers à un endroit spécifique.

### Conditions préalables

Privilège nécessaire : **Banque de données.Parcourir la banque de donnée**

### Procédure

- 1 Cliquez sur **Stockage** dans l'inventaire VMware Host Client et cliquez sur **Banques de données**.
- 2 Cliquez sur **Explorateur de banque de données**.
- 3 Cliquez sur **Créer un répertoire**.
- 4 Sélectionnez la banque de données cible.
- 5 (Facultatif) Entrez un nom pour le nouveau répertoire.
- 6 Cliquez sur **Créer un répertoire**.
- 7 Cliquez sur **Fermer** pour quitter le navigateur.

## Renommer une banque de données dans VMware Host Client

Vous pouvez modifier le nom d'affichage d'une banque de données dans VMware Host Client.

---

**Note** Si l'hôte est géré par vCenter Server, vous ne pouvez pas renommer la banque de données dans VMware Host Client. Vous pouvez uniquement effectuer cette tâche à partir de l'instance de vCenter Server qui gère l'hôte.

---

### Procédure

- 1 Cliquez sur **Stockage** dans l'inventaire VMware Host Client et cliquez sur **Banques de données**.
- 2 Cliquez avec le bouton droit sur une banque de données de la liste et sélectionnez **Renommer** dans le menu contextuel.
- 3 Entrez un nom pour la banque de données et cliquez sur **Enregistrer** pour appliquer les modifications.
- 4 (Facultatif) Cliquez sur **Actualiser** pour voir le nouveau nom de la banque de données dans la liste des banques de données disponibles.

## Supprimer une banque de données VMFS dans VMware Host Client

Vous pouvez supprimer n'importe quel type de banque de données VMFS, y compris les copies que vous avez montées sans nouvelle signature. Lorsque vous supprimez une banque de données, la banque de données et tous les fichiers associés à la banque de données sont supprimés de l'hôte.

---

**Note** L'opération de suppression de la banque de données supprime définitivement tous les fichiers associés aux machines virtuelles de la banque de données. Bien que vous puissiez supprimer la banque de données sans la démonter, il est préférable de la démonter au préalable.

---

### Conditions préalables

Supprimez toutes les machines virtuelles de la banque de données.

### Procédure

- 1 Cliquez sur **Stockage** dans l'inventaire VMware Host Client et cliquez sur **Banques de données**.
- 2 Cliquez avec le bouton droit sur la banque de données de la liste et sélectionnez **Supprimer** dans le menu déroulant.
- 3 Cliquez sur **Confirmer** pour supprimer la banque de données.

## Provisionnement dynamique du stockage dans VMware Host Client

Avec ESXi, vous pouvez utiliser deux modèles de provisionnement dynamique, au niveau de la baie et au niveau du disque virtuel.

Le provisionnement dynamique est une méthode qui optimise l'utilisation du stockage en allouant un espace de stockage de manière flexible, à la demande. Le provisionnement dynamique s'oppose au modèle traditionnel, appelé provisionnement statique. Avec le provisionnement statique, une quantité importante d'espace de stockage est prévue à l'avance en prévision des futurs besoins de stockage. Toutefois, l'espace pourrait rester inutilisé et entraîner une sous-utilisation de la capacité de stockage.

Les fonctionnalités de provisionnement dynamique de VMware vous permettent d'éliminer les problèmes de sous-utilisation de stockage au niveau de la banque de données et au niveau de la baie de stockage.

## Créer des disques virtuels à provisionnement dynamique dans VMware Host Client

Pour économiser de l'espace de stockage, vous pouvez créer des disques virtuels à provisionnement dynamique. Le disque virtuel alloué dynamiquement démarre avec une petite taille et grandit au fur et à mesure que de l'espace disque est nécessaire. Vous pouvez créer des disques alloués dynamiquement uniquement sur les banques de données qui prennent en charge l'provisionnement dynamique au niveau du disque.

La procédure suivante suppose que vous créez une nouvelle machine virtuelle. Pour plus d'informations, consultez [Créer une machine virtuelle dans VMware Host Client](#).

#### Procédure

- 1 Cliquez avec le bouton droit sur **Hôte** dans l'inventaire VMware Host Client et sélectionnez **Créer/Enregistrer VM**.  
L'assistant **Nouvelle machine virtuelle** s'ouvre.
- 2 Sélectionnez une méthode pour ajouter une nouvelle machine virtuelle à l'hôte et cliquez sur **Suivant**.
- 3 Entrez un nom pour votre machine virtuelle.
- 4 Sélectionnez la compatibilité de la machine virtuelle dans le menu déroulant **Compatibilité**.
- 5 Sélectionnez une version du système d'exploitation invité dans le menu déroulant **Version du SE invité** et cliquez sur **Suivant**.
- 6 Dans la liste des banques de données accessibles, sur la page Sélectionner le stockage de l'assistant **Nouvelle machine virtuelle**, cliquez sur la banque de données de destination pour les fichiers de configuration de la machine virtuelle et tous les disques virtuels.
- 7 Sous l'onglet **Matériel virtuel**, développez **Disque dur**.
- 8 Sous **Provisionnement de disque**, sélectionnez le bouton-radio **Provisionnement dynamique** et cliquez sur **Suivant**.
- 9 Sur la page Prêt à terminer de l'assistant **Nouvelle machine virtuelle**, passez en revue les paramètres de configuration pour la machine virtuelle et cliquez sur **Terminer** pour enregistrer vos paramètres.

### Afficher des ressources de stockage de machine virtuelle dans VMware Host Client

Vous pouvez consulter comment l'espace de stockage est alloué pour vos machines virtuelles dans VMware Host Client.

La consommation des ressources 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.

Pour les machines virtuelles avec des disques alloués dynamiquement, la valeur réelle d'utilisation du stockage peut être inférieure à la taille du disque virtuel.

#### Procédure

- 1 Cliquez sur la machine virtuelle dans l'inventaire VMware Host Client.
- 2 Consultez les informations sur la consommation des ressources dans la partie inférieure droite de la page de résumé de la machine virtuelle.

## Déterminer le format de disque d'une machine virtuelle dans VMware Host Client

Vous pouvez déterminer si votre disque virtuel est provisionné au format dynamique ou statique.

### Procédure

- 1 Cliquez avec le bouton droit de la souris sur la machine virtuelle dans l'inventaire VMware Host Client et sélectionnez **Modifier les paramètres**.
- 2 Sous l'onglet **Matériel virtuel**, développez **Disque dur**.

La zone de texte **Type** affiche le format de votre disque virtuel.

## Gestion des adaptateurs de stockage dans VMware Host Client

Lorsque vous vous connectez à un hôte ou à vCenter Server à l'aide de VMware Host Client, vous pouvez exécuter plusieurs tâches sur vos adaptateurs de stockage, comme configurer plusieurs composants iSCSI.

Lorsque vous activez iSCSI sur l'hôte que vous gérez dans votre environnement VMware Host Client, vous pouvez configurer et ajouter de nouvelles liaisons de port réseau, ainsi que des cibles statique et dynamique, vous pouvez gérer l'authentification CHAP et configurer divers paramètres avancés sur votre stockage hôte.

### Afficher les adaptateurs de stockage dans VMware Host Client

Affichez les adaptateurs de stockage que votre hôte utilise et les informations associées.

#### Procédure

- 1 Cliquez sur **Stockage** dans l'inventaire VMware Host Client et cliquez sur **Adaptateurs**.  
Tous les adaptateurs de stockage disponibles pour l'hôte sont répertoriés dans **Adaptateurs**.
- 2 Pour afficher les détails d'un adaptateur spécifique, sélectionnez-le dans la liste.

### Configuration d'adaptateurs iSCSI logiciels dans VMware Host Client

L'implémentation du protocole iSCSI logiciel vous permet d'utiliser des cartes réseau standard pour connecter votre hôte à une cible iSCSI distante sur le réseau IP. L'adaptateur iSCSI logiciel qui est intégré dans l'ESXi communique avec les cartes réseau physiques via la pile réseau.

---

**Note** Avant d'utiliser l'adaptateur iSCSI logiciel, vous devez d'abord installer le réseau, activer l'adaptateur et configurer les paramètres tels que le CHAP.

---

Le workflow de configuration de l'adaptateur iSCSI inclut les procédures suivantes :

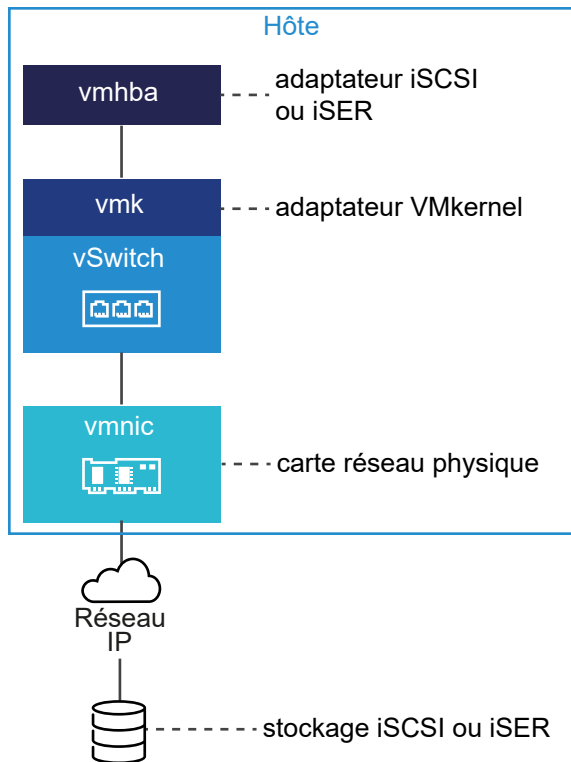
- Activation d'iSCSI sur votre hôte. Reportez-vous à la section [Activer iSCSI pour un hôte ESXi dans VMware Host Client](#).

- Ajout d'une liaison de port. Reportez-vous à la section [Ajouter une liaison de port dans VMware Host Client](#).
- Suppression d'une liaison de port. Reportez-vous à la section [Supprimer une liaison de port dans VMware Host Client](#).

## Configuration du réseau pour iSCSI et iSER

Certains types d'adaptateurs iSCSI dépendent de la mise en réseau VMkernel. Il s'agit notamment des adaptateurs iSCSI logiciels, des adaptateurs iSCSI matériels dépendants et des adaptateurs iSER (VMware iSCSI sur RDMA). Si votre environnement inclut l'un de ces adaptateurs, vous devez configurer les connexions pour le trafic entre le composant iSCSI ou iSER et les adaptateurs réseau physiques.

La configuration de la connexion réseau implique de créer un adaptateur virtuel VMkernel pour chaque adaptateur réseau physique, d'utiliser le mappage 1:1 entre chaque adaptateur réseau physique et virtuel, puis d'associer l'adaptateur VMkernel à un adaptateur iSCSI ou iSER approprié. Ce processus porte le nom de liaison de port.



Lorsque vous configurez la liaison de port, suivez ces règles :

- Vous pouvez connecter l'adaptateur iSCSI logiciel n'importe quelle carte réseau physique disponible sur votre hôte.
- Les adaptateurs iSCSI dépendants doivent uniquement être connectés à leurs propres cartes réseau physiques.
- Vous devez connecter l'adaptateur iSER uniquement à l'adaptateur réseau compatible RDMA.

Pour des considérations spécifiques sur la manière d'utiliser les connections du réseau avec un adaptateur iSCSI logiciel, reportez-vous à l'article de la base de connaissances VMware à l'adresse <http://kb.vmware.com/kb/2038869>.

## Activer iSCSI pour un hôte ESXi dans VMware Host Client

Activez iSCSI pour votre hôte dans votre environnement VMware Host Client afin de configurer les paramètres des adaptateurs de stockage, tels que l'authentification CHAP, les liaisons de port réseau, les cibles statique et dynamique et d'autres paramètres avancés.

### Procédure

- 1 Cliquez sur **Stockage** dans l'inventaire VMware Host Client, cliquez sur **Adaptateurs**, puis sur **Configurer iSCSI**.
- 2 Sélectionnez la case d'option **Activé**.
- 3 (Facultatif) Configurez les paramètres et composants que vous souhaitez modifier.
- 4 Cliquez sur **Enregistrer la configuration**.

## Recommandations pour la configuration de la mise en réseau avec un iSCSI logiciel

Lorsque vous configurez la mise en réseau avec un iSCSI logiciel, vous devez tenir compte de plusieurs recommandations.

### Liaison de port iSCSI logicielle

Vous pouvez lier l'initiateur iSCSI logiciel sur l'hôte ESXi à un ou plusieurs ports VMkernel afin que le trafic iSCSI emprunte toujours exclusivement les ports liés. Les ports non liés ne sont pas utilisés pour le trafic iSCSI.

Lorsque la liaison de port est configurée, l'initiateur iSCSI crée des sessions iSCSI allant de tous les ports liés vers tous les portails cibles configurés.

Consultez les exemples suivants.

| Ports VMkernel        | Portails cibles   | Sessions iSCSI     |
|-----------------------|-------------------|--------------------|
| 2 ports VMkernel liés | 2 portails cibles | 4 sessions (2 x 2) |
| 4 ports VMkernel liés | 1 portail cible   | 4 sessions (4 x 1) |
| 2 ports VMkernel liés | 4 portails cibles | 8 sessions (2 x 4) |

**Note** Assurez-vous que tous les portails cibles peuvent être atteints à partir de tous les ports VMkernel lorsque la liaison de port est utilisée, sans quoi les sessions iSCSI risquent de ne pas être créées. Il en résulte que l'opération de réanalyse peut prendre plus de temps que prévu.



## Absence de liaison de port

Si vous n'utilisez pas la liaison de port, la couche de mise en réseau ESXi sélectionne le meilleur port VMkernel en fonction de sa table de routage. L'hôte utilise le port pour créer une session iSCSI avec le portail cible. En l'absence de liaison de port, une seule session est créée pour chaque portail cible.

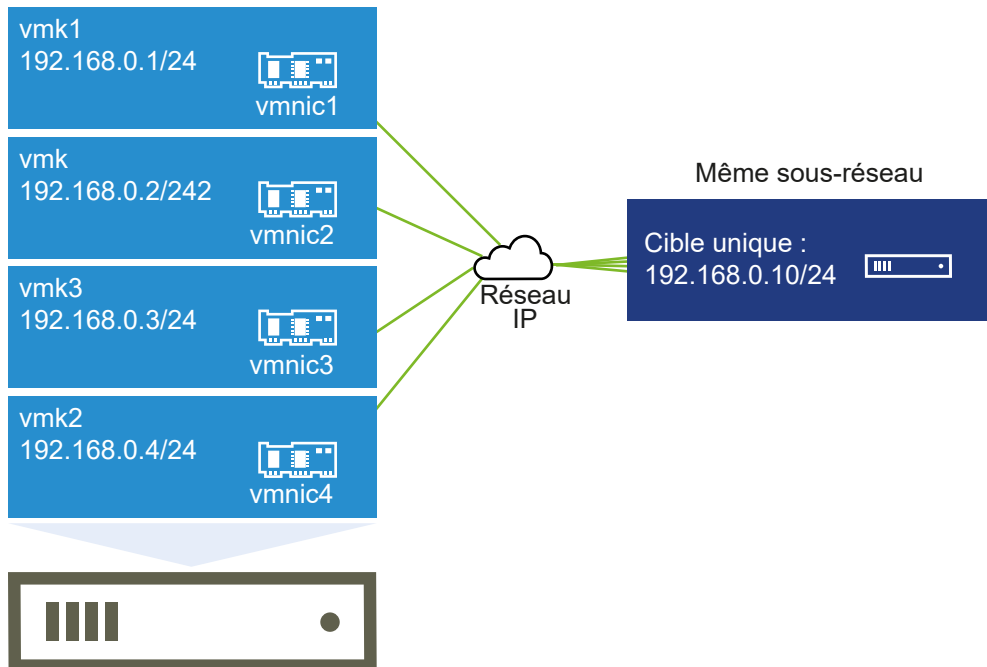
Consultez les exemples suivants.

| Ports VMkernel            | Portails cibles   | Sessions iSCSI |
|---------------------------|-------------------|----------------|
| 2 ports VMkernel non liés | 2 portails cibles | 2 sessions     |
| 4 ports VMkernel non liés | 1 portail cible   | 1 session      |
| 2 ports VMkernel non liés | 4 portails cibles | 4 sessions     |

## Chemins multiples avec iSCSI logiciel

Exemple 1. Chemins multiples vers une cible iSCSI avec un portail réseau unique

Si votre cible n'a qu'un portail réseau, vous pouvez créer plusieurs chemins vers la cible en ajoutant plusieurs ports VMkernel à votre hôte ESXi et en les liant à l'initiateur iSCSI.

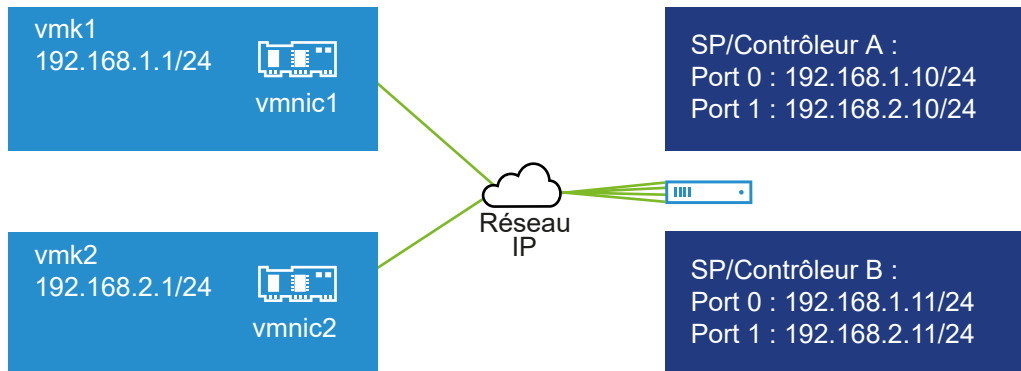


Dans cet exemple, tous les ports initiateurs et le portail cible sont configurés sur le même sous-réseau. La cible peut être atteinte par l'intermédiaire de tous les ports liés. Vous disposez de quatre ports VMkernel et d'un portail cible, de sorte que quatre chemins en tout sont créés.

Sans la liaison de port, un seul chemin est créé.

Exemple 2. Chemins multiples avec des ports VMkernel sur différents sous-réseaux

Vous pouvez créer plusieurs chemins en configurant plusieurs ports et portails cibles sur des sous-réseaux IP différents. En maintenant le port initiateur et le port cible sur des sous-réseaux différents, vous pouvez obliger ESXi à créer des chemins passant par des ports spécifiques. Dans cette configuration, vous n'utilisez pas la liaison de port, car celle-ci nécessite que tous les ports initiateurs et cibles se trouvent sur le même sous-réseau.



ESXi sélectionne vmmk1 lors de la connexion au Port 0 du Contrôleur A et du Contrôleur B, car ces trois ports se trouvent tous sur le même sous-réseau. De même, vmmk2 est sélectionné lors de la connexion au Port 1 du Contrôleur A et du Contrôleur B. Dans cette configuration, vous pouvez utiliser l'association de cartes réseau.

En tout, quatre chemins sont créés.

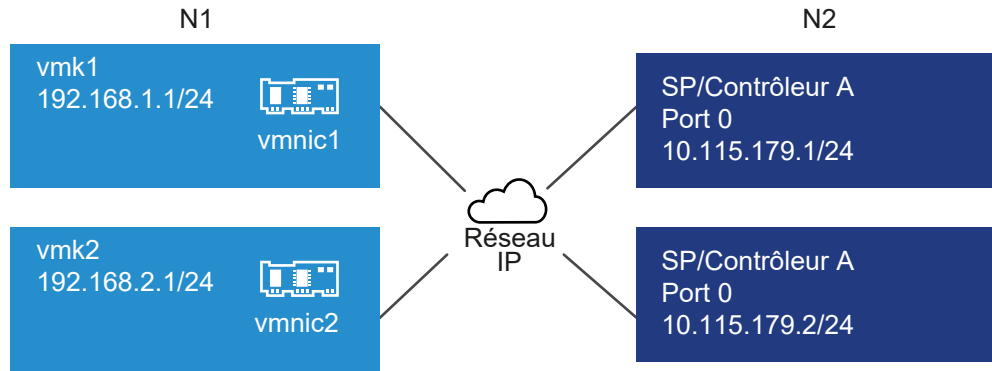
| Chemins  | Description                    |
|----------|--------------------------------|
| Chemin 1 | vmmk1 et Port0 du Contrôleur A |
| Chemin 2 | vmmk1 et Port0 du Contrôleur B |
| Chemin 3 | vmmk2 et Port1 du Contrôleur A |
| Chemin 4 | vmmk2 et Port1 du Contrôleur B |

### Routage avec iSCSI logiciel

Vous pouvez utiliser la commande `esxcli` pour ajouter des routes statiques pour votre trafic iSCSI. Une fois que vous avez configuré des routes statiques, les ports initiateur et cible sur différents sous-réseaux peuvent communiquer entre eux.

Exemple 1. Utilisation de routes statiques avec liaison de port

Dans cet exemple, vous maintenez tous les ports VMkernel liés dans un sous-réseau (N1) et vous configurez tous les portails cibles dans un autre sous-réseau (N2). Vous pouvez alors ajouter une route statique pour le sous-réseau cible (N2).

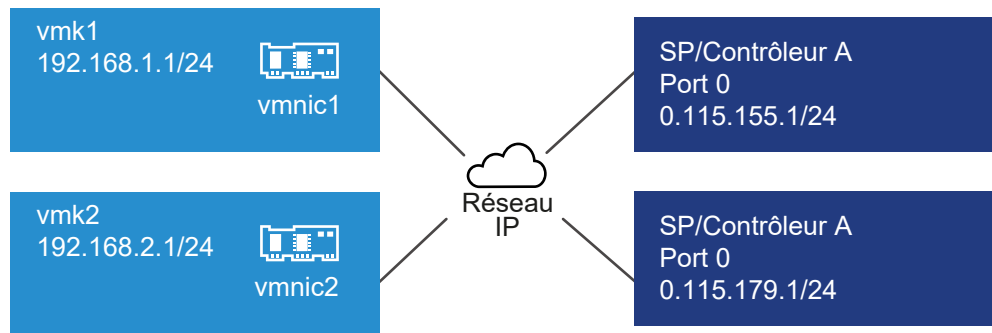


Utilisez la commande suivante :

```
# esxcli network ip route ipv4 add -gateway 192.168.1.253 -network 10.115.179.0/24
```

Exemple 2. Utilisation de routes statiques pour créer plusieurs chemins

Dans cette configuration, vous utilisez le routage statique lorsque vous employez des sous-réseaux différents. La liaison de port ne peut pas être utilisée avec cette configuration.



Vous configurez vmk1 et vmk2 dans des sous-réseaux différents, à savoir 192.168.1.0 et 192.168.2.0. Vos portails cibles se trouvent également dans des sous-réseaux distincts, 10.115.155.0 et 10.115.179.0.

Vous pouvez ajouter la route statique vers 10.115.155.0 à partir de vmk1. Assurez-vous que la passerelle peut être atteinte à partir de vmk1.

```
# esxcli network ip route ipv4 add -gateway 192.168.1.253 -network 10.115.155.0/24
```

Vous ajoutez ensuite la route statique vers 10.115.179.0 à partir de vmk2. Assurez-vous que la passerelle peut être atteinte à partir de vmk2.

```
# esxcli network ip route ipv4 add -gateway 192.168.2.253 -network 10.115.179.0/24
```

Lors d'une connexion à l'aide du Port 0 du Contrôleur A, vmk1 est utilisé.

Lors d'une connexion à l'aide du Port 0 du Contrôleur B, vmk2 est utilisé.

### Exemple 3. Routage avec une passerelle distincte par port vmkernel

À partir de vSphere 6.5, vous pouvez configurer une passerelle distincte par port VMkernel. Si vous utilisez le DHCP pour obtenir la configuration IP d'un port VMkernel, il est également possible d'obtenir des informations sur la passerelle à l'aide du DHCP.

Pour afficher les informations sur la passerelle par port VMkernel, utilisez la commande suivante :

```
# esxcli network ip interface ipv4 address list
```

| Name | IPv4 Address   | IPv4 Netmask  | IPv4 Broadcast | Address Type | Gateway        | DHCP  | DNS   |
|------|----------------|---------------|----------------|--------------|----------------|-------|-------|
| ---- | -----          | -----         | -----          | -----        | -----          | ----- | ----- |
| vmk0 | 10.115.155.122 | 255.255.252.0 | 10.115.155.255 | DHCP         | 10.115.155.253 | true  |       |
| vmk1 | 10.115.179.209 | 255.255.252.0 | 10.115.179.255 | DHCP         | 10.115.179.253 | true  |       |
| vmk2 | 10.115.179.146 | 255.255.252.0 | 10.115.179.255 | DHCP         | 10.115.179.253 | true  |       |

Lorsque vous disposez de passerelles distinctes pour chaque port VMkernel, vous utilisez la liaison de port pour atteindre des cibles dans différents sous-réseaux.

## Ajouter une liaison de port dans VMware Host Client

Utilisez VMware Host Client pour lier un adaptateur iSCSI à un adaptateur VMkernel sur votre hôte.

### Conditions préalables

- Créez un adaptateur VMkernel virtuel pour chaque adaptateur réseau physique sur votre hôte. Si vous utilisez plusieurs adaptateurs VMkernel, configurez une stratégie réseau appropriée.
- Privilège nécessaire : **Hôte.Configuration.Configuration de la partition de stockage**

### Procédure

- 1 Cliquez sur **Stockage** dans l'inventaire VMware Host Client, cliquez sur **Adaptateurs**, puis sur **Configurer iSCSI**.
- 2 Dans la section **Liaisons de port réseau**, cliquez sur **Ajouter une liaison de port**.
- 3 Sélectionnez un adaptateur VMkernel à relier à l'adaptateur iSCSI.

**Note** Assurez-vous que la stratégie réseau de l'adaptateur VMkernel est conforme aux conditions de liaison.

Vous pouvez lier l'adaptateur iSCSI logiciel à un ou plusieurs adaptateurs VMkernel. S'il s'agit d'un adaptateur iSCSI matériel dépendant, seul un adaptateur VMkernel associé à la carte réseau physique appropriée est disponible.

- 4 Cliquez sur **Sélectionner**.
- 5 Cliquez sur **Enregistrer la configuration**.

## Supprimer une liaison de port dans VMware Host Client

Modifier la configuration iSCSI sur votre hôte pour supprimer une liaison de port.

**Procédure**

- 1 Cliquez sur **Stockage** dans l'inventaire VMware Host Client, cliquez sur **Adaptateurs**, puis sur **Configurer iSCSI**.
- 2 Dans la section **Liaisons de port réseau**, sélectionnez une NIC VMkernel dans la liste.
- 3 Cliquez sur **Supprimer la liaison de port**.
- 4 Cliquez sur **Enregistrer la configuration**.

**Configurer une cible dynamique dans VMware Host Client**

Vous devez configurer les adresses de découverte de cible pour que l'adaptateur iSCSI puisse identifier les ressources de stockage du réseau qui sont accessibles. L'hôte ESXi prend en charge les méthodes de détection dynamique et statique. Avec la découverte dynamique, chaque fois que l'initiateur contacte un système de stockage iSCSI en particulier, il envoie la demande SendTargets au système iSCSI. Le système iSCSI répond en fournissant une liste de cibles disponibles à l'initiateur.

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'une analyse se produira, que le HBA se réinitialisera ou que l'hôte redémarrera.

---

**Note** Avec un iSCSI logiciel ou matériel dépendant, ESXi filtre les adresses cibles selon la famille IP de l'adresse de serveur iSCSI spécifiée. S'il s'agit d'une adresse IPv4, les adresses IPv6 susceptible d'apparaître dans la réponse SendTargets provenant du serveur iSCSI sont filtrées. Lorsqu'un serveur iSCSI est spécifié par le biais de noms DNS ou que la réponse SendTargets du serveur iSCSI contient des noms DNS, ESXi utilise la famille IP de la première entrée résolue dans la recherche DNS.

---

Lorsque vous configurez la découverte dynamique, vous pouvez seulement ajouter un nouveau système iSCSI. Vous ne pouvez pas changer l'adresse IP, le nom DNS ni le numéro de port d'un système iSCSI existant. Pour modifier ces paramètres, supprimez le système existant et ajoutez-en un nouveau.

**Conditions préalables**

Privilège nécessaire : **Hôte.Configuration.Configuration de la partition de stockage**

**Procédure**

- 1 Cliquez sur **Stockage** dans l'inventaire VMware Host Client, cliquez sur **Adaptateurs**, puis sur **Configurer iSCSI**.
- 2 Cliquez sur **Ajouter une cible dynamique**.

La nouvelle cible dynamique figure dans la liste.

- 3 Pour ajouter une adresse à la nouvelle cible dynamique, cliquez sur la cible dans la liste et saisissez l'adresse.
- 4 (Facultatif) Pour modifier le numéro de port de la nouvelle cible dynamique, cliquez sur la zone de texte **Port** de la cible et saisissez le nouveau numéro de port.
- 5 (Facultatif) Pour modifier les paramètres de la cible dynamique, sélectionnez la nouvelle cible dans la liste des cibles disponibles, cliquez sur **Modifier les paramètres**, configurez les paramètres que vous souhaitez modifier, puis cliquez sur **Enregistrer**.
- 6 (Facultatif) Pour supprimer une cible précise, sélectionnez-la et cliquez sur **Supprimer la cible dynamique**.

La cible ne figure plus dans la liste des cibles dynamiques.

- 7 Cliquez sur **Enregistrer la configuration**.

## Configurer une cible statique dans VMware Host Client

Avec les initiateurs iSCSI, vous pouvez utiliser la découverte statique pour saisir manuellement les informations pour les cibles.

Quand vous configurez la découverte statique, vous pouvez uniquement ajouter de nouvelles 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.

Outre la méthode de découverte dynamique, vous pouvez utiliser la découverte statique et entrer manuellement des informations pour les cibles. L'adaptateur iSCSI s'appuie sur une liste de cibles que vous spécifiez pour contacter les serveurs iSCSI et communiquer avec eux.

### Conditions préalables

Privilèges nécessaires : **Hôte.Configuration.Configuration de la partition de stockage**

### Procédure

- 1 Cliquez sur **Stockage** dans l'inventaire VMware Host Client, cliquez sur **Adaptateurs**, puis sur **Configurer iSCSI**.
- 2 Cliquez sur **Ajouter une cible statique**.  
La nouvelle cible statique figure dans la liste.
- 3 Pour ajouter un nom à la nouvelle cible statique, cliquez sur la cible dans la liste et saisissez le nom.
- 4 Pour ajouter une adresse à la nouvelle cible statique, cliquez sur la cible dans la liste et tapez l'adresse.
- 5 (Facultatif) Pour modifier le numéro de port de la nouvelle cible statique, cliquez sur la zone de texte **Port** de la cible et tapez le nouveau numéro de port.

- 6 (Facultatif) Pour modifier les paramètres de la cible statique, sélectionnez la nouvelle cible dans la liste des cibles disponibles, cliquez sur **Modifier les paramètres**, configurez les paramètres que vous souhaitez modifier, puis cliquez sur **Enregistrer**.
- 7 (Facultatif) Pour supprimer une cible précise, sélectionnez-la et cliquez sur **Supprimer la cible statique**.

La cible ne figure plus dans la liste des cibles statiques existantes.

- 8 Cliquez sur **Enregistrer la configuration**.

## Modifier les paramètres avancés d'iSCSI dans VMware Host Client

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, il est inutile de modifier ces paramètres, car votre hôte fonctionne avec les valeurs prédéfinies assignées.

---

**Attention** Ne modifiez aucun paramètre iSCSI avancé à moins de travailler avec l'équipe du support VMware ou de disposer par d'autres biais, d'informations précises sur les valeurs à attribuer pour la modification de paramètres.

---

### Conditions préalables

Privlège nécessaire : **Hôte.Configuration.Configuration de la partition de stockage**

### Procédure

- 1 Cliquez sur **Stockage** dans l'inventaire VMware Host Client, cliquez sur **Adaptateurs**, puis sur **Configurer iSCSI**.
- 2 Cliquez sur **Paramètres avancés** pour afficher la liste complète des paramètres.
- 3 Modifiez les paramètres souhaités, puis cliquez sur **Enregistrer la configuration**.

## Configurer l'authentification CHAP pour un adaptateur iSCSI dans VMware Host Client

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.

Le nom CHAP doit comporter moins de 511 caractères alphanumériques et le secret CHAP doit comporter moins de 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.

## Conditions préalables

- Avant de configurer des paramètres CHAP pour les adaptateurs iSCSI logiciel ou matériel dépendants, déterminez si vous devez configurer un CHAP unilatéral, également appelé normal, ou un CHAP mutuel. Les adaptateurs iSCSI matériels indépendants n'admettent pas le CHAP mutuel.

- En CHAP unilatéral, la cible authentifie l'initiateur.
- Dans la méthode CHAP mutuelle, la cible et l'initiateur s'authentifient mutuellement. Utilisez des secrets différents pour la méthode CHAP et pour la méthode CHAP mutuelle.

Lorsque vous définissez les paramètres CHAP, vérifiez qu'ils correspondent aux paramètres du stockage.

- Privilèges nécessaires : **Hôte.Configuration.Configuration de la partition de stockage**

## Procédure

- 1 Cliquez sur **Stockage** dans l'inventaire VMware Host Client, cliquez sur **Adaptateurs**, puis sur **Configurer iSCSI**.
- 2 Pour configurer un CHAP unilatéral, développez l'**authentification CHAP** de manière à afficher tous les paramètres.
  - a Sélectionnez le niveau de sécurité CHAP.
  - b Saisir le nom CHAP.  
Assurez-vous que le nom que vous indiquez concorde avec celui configuré côté stockage.
  - c Saisissez un secret CHAP unilatéral à utiliser pour l'authentification. Utilisez le même secret que celui que vous entrez côté stockage.
- 3 Pour configurer un CHAP mutuel, sélectionnez **Utiliser CHAP** comme option de CHAP unilatéral. Développez **Authentification CHAP mutuelle** pour afficher tous les paramètres.
  - a Cochez **Utiliser CHAP**.
  - b Tapez le nom CHAP mutuel.
  - c Tapez le secret CHAP mutuel.  
Utilisez des secrets différents pour la méthode CHAP unilatérale et pour la méthode CHAP mutuelle.
- 4 Cliquez sur **Enregistrer la configuration**.

## Résultats

Si vous modifiez les paramètres d'authentification d'un adaptateur iSCSI, vous pouvez uniquement utiliser les informations d'identification actualisées pour les nouvelles sessions iSCSI. Les sessions existantes persistent jusqu'à ce que la connexion soit perdue en raison d'un facteur extérieur tel qu'une ré-authentification forcée, ou que vous supprimiez et ajoutiez les cibles iSCSI de l'adaptateur.



# Gestion des périphériques de stockage dans VMware Host Client

Vous pouvez utiliser VMware Host Client pour gérer les périphériques de stockage locaux et en réseau auxquels l'hôte ESXi que vous gérez a accès.

## Afficher les périphériques de stockage dans VMware Host Client

Affichez tous les périphériques de stockage disponibles pour un hôte. Si vous utilisez des plug-ins chemins multiples tiers, les périphériques de stockage disponibles via les plug-ins apparaissent également dans la liste.

La vue Périphériques de stockage vous permet de répertorier les périphériques de stockage des hôtes, d'analyser leurs informations et de modifier leurs propriétés.

### Procédure

- 1 Cliquez sur **Stockage** dans l'inventaire VMware Host Client et cliquez sur **Périphériques**.

Tous les périphériques de stockage disponibles pour l'hôte sont répertoriés dans **Périphériques**.

- 2 Pour afficher les détails d'un périphérique spécifique, sélectionnez-le dans la liste.

## Effacer une table de partition de périphérique dans VMware Host Client

Lorsque vous êtes connecté à un hôte ESXi avec VMware Host Client, vous pouvez effacer la table de partition d'un périphérique disque accessible depuis l'hôte.

### Conditions préalables

Vérifiez que le périphérique n'est pas utilisé par ESXi comme disque de démarrage, banque de données VMFS ou vSAN.

### Procédure

- 1 Cliquez sur **Stockage** dans VMware Host Client et cliquez sur **Périphériques**.
- 2 Cliquez avec le bouton droit sur un périphérique de la liste, cliquez sur **Effacer la table de partition** et cliquez sur **Oui**.

L'effacement de la table de partition peut provoquer la perte de données.

## Modifier individuellement des partitions de périphériques dans VMware Host Client

Lorsque vous vous connectez à un hôte ESXi avec VMware Host Client, vous pouvez supprimer les partitions individuelles d'un périphérique en utilisant l'éditeur de partitions.

### Conditions préalables

Vérifiez que le périphérique n'est pas utilisé par ESXi comme disque de démarrage, banque de données VMFS ou vSAN.

### Procédure

- 1 Cliquez sur **Stockage** dans VMware Host Client et cliquez sur **Périphériques**.
- 2 Cliquez avec le bouton droit sur un périphérique dans la liste, puis cliquez sur **Modifier les partitions**.
- 3 Sélectionnez une partition et cliquez sur **Supprimer la partition**.
- 4 (Facultatif) Cliquez sur **Réinitialiser** pour restaurer les partitions d'origine.
- 5 Cliquez sur **Enregistrer les partitions**.
- 6 Confirmez que vous souhaitez modifier la partition.

## Gestion de la mémoire persistante

ESXi 6.7 et versions ultérieures prend en charge la technologie de mémoire informatique la plus récente, qui est appelée mémoire non volatile (NVM) ou mémoire persistante (PMem). La PMem associe le taux de transfert de données élevé de la mémoire volatile de l'ordinateur avec la persistance et la résilience de stockage traditionnel. Les périphériques PMem ont une latence d'accès inférieure et peuvent conserver les données stockées au moyen de redémarrages ou de pannes de courant.

### Modes de consommation des ressources de mémoire persistante de l'hôte

Lorsque vous ajoutez un périphérique PMem physique à un hôte, ESXi détecte la ressource PMem et l'expose en tant que banque de données PMem locale au niveau de l'hôte pour les machines virtuelles qui s'exécutent sur l'hôte. En fonction du système d'exploitation invité, les machines virtuelles peuvent avoir un accès direct aux ressources PMem.

Chaque hôte ne peut avoir qu'une seule banque de données PMem locale pour regrouper et représenter toutes les ressources PMem de l'hôte.

La mémoire persistante associe les propriétés de la mémoire et du stockage. Par conséquent, les machines virtuelles peuvent consommer les ressources PMem de l'hôte ESXi sous forme de mémoire (par le biais de périphériques NVDIMM virtuels) ou de stockage (par le biais de disques durs PMem virtuels).

La banque de données PMem locale au niveau de l'hôte stocke tous les périphériques NVDIMM et les disques durs PMem virtuels à accès direct.

## Mémoire persistante virtuelle (vPMem)

Lorsque ce mode est activé, si le système d'exploitation invité prend en charge les périphériques PMem, la machine virtuelle peut avoir un accès direct aux ressources PMem physiques de l'hôte et les utiliser comme mémoire standard adressable en octets.

Les machines virtuelles utilisent des modules NVDIMM virtuels pour un accès direct à la mémoire persistante. Un module NVDIMM est un périphérique de mémoire qui se trouve sur un canal de mémoire ordinaire, mais qui contient de la mémoire non volatile. Dans vSphere 6.7, le NVDIMM virtuel est un nouveau type de périphérique qui représente les régions PMem physiques de l'hôte. Une machine virtuelle unique peut compter jusqu'à 64 périphériques NVDIMM virtuels. Chaque périphérique NVDIMM est stocké sur la banque de données PMem locale au niveau de l'hôte.

---

**Note** Pour ajouter un périphérique NVDIMM à une machine virtuelle, celle-ci doit être de version de matériel 14 et le système d'exploitation invité doit prendre en charge la mémoire persistante. Si le système d'exploitation invité ne prend pas en charge la mémoire persistante, vous pouvez toujours utiliser PMem, mais vous ne pouvez pas ajouter de périphérique NVDIMM à la machine virtuelle.

---

## Disques PMem virtuels (vPMemDisk)

Lorsque ce mode est activé, la machine virtuelle ne dispose pas d'un accès direct aux ressources PMem de l'hôte.

Vous devez ajouter un disque dur PMem virtuel à la machine virtuelle. Un disque dur PMem virtuel est un disque SCSI traditionnel auquel la stratégie de stockage PMem est appliquée. La stratégie place automatiquement le disque dur sur la banque de données PMem locale au niveau de l'hôte.

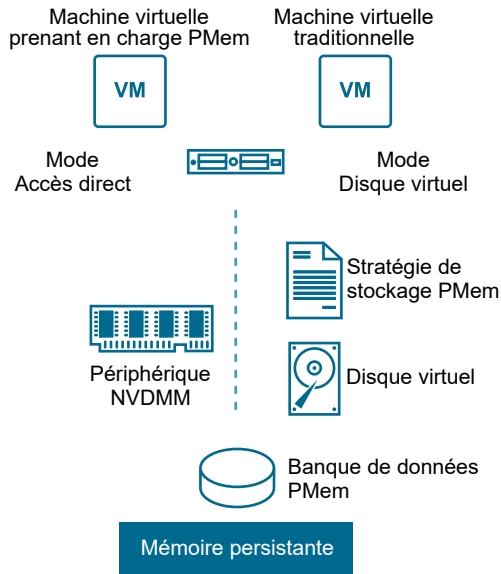
Lorsque ce mode d'utilisation est activé, il n'existe pas de configuration requise pour la version de matériel de la machine virtuelle et du système d'exploitation invité.

---

**Note** Si le système d'exploitation invité ne prend pas en charge la mémoire persistante, les machines virtuelles peuvent l'utiliser uniquement via les disques vPMemDisks.

---

Le diagramme suivant illustre l'interaction des composants de mémoire persistante.



Pour plus d'informations sur la configuration et la gestion de machines virtuelles dotées de modules NVDIMM ou de disques à mémoire persistante virtuels, consultez la documentation *Gestion des ressources vSphere*.

## Structure de la banque de données PMem

L'interface utilisateur VMware Host Client fournit des informations sur la structure complexe de la banque de données PMem locale au niveau de l'hôte. Pour analyser ces informations et les utiliser à des fins de dépannage et de gestion, vous devez être familiarisé avec les concepts liés à cette structure complexe.

### Modules

Dans l'interface utilisateur VMware Host Client, les modules représentent les NVDIMM physiques connectés à la carte mère de l'hôte.

Dans VMware Host Client, vous pouvez vérifier l'état de santé de chaque module et identifier les modules NVDIMM défectueux.

### Ensembles d'entrelacements

Les ensembles d'entrelacements sont des regroupements logiques d'un ou de plusieurs modules. Les ensembles d'entrelacements révèlent de quelle manière les informations sont réparties sur les DIMM physiques et comment ESXi lit ces informations à partir des modules. Du fait que ESXi effectue la lecture à partir de chaque ensemble d'entrelacements successivement, ceux-ci permettent d'obtenir un débit de mémoire plus élevé.

Par exemple, si un ensemble d'entrelacements comprend deux modules, ESXi lit les informations sur les deux DIMM physiques en parallèle, puis passe à l'ensemble d'entrelacements suivant.

L'interface utilisateur de VMware Host Client fournit des informations sur la manière dont les NVDIMM sont regroupés sous forme d'ensembles d'entrelacements.

## Espaces de noms

Les espaces de noms sont des régions de plages de mémoire traitées de façon contiguë dans le NVDIMM. Les espaces de noms peuvent parcourir les ensembles d'entrelacements. La banque de données PMem s'appuie sur les espaces de noms.

Dans VMware Host Client, vous pouvez afficher la capacité, l'état de santé et l'ID de l'emplacement de chaque espace de noms.

## Afficher les informations relatives aux modules, aux ensembles d'entrelacement et aux espaces de noms dans VMware Host Client

Dans VMware Host Client, vous pouvez afficher plus d'informations sur les modules, les ensembles d'entrelacement et l'espace de noms de la banque de données PMem hôte-locale. Vous pouvez ainsi facilement identifier un module défectueux et effectuer un dépannage.

Vous ne pouvez pas effectuer la plupart des tâches de gestion de banque de données traditionnelles sur la banque de données PMem hôte-locale. En revanche, vous pouvez utiliser les informations relatives aux modules, aux ensembles d'entrelacement et aux espaces de noms à des fins de dépannage.

### Conditions préalables

Vérifiez que l'hôte dispose d'au moins un périphérique NVDIMM physique.

### Procédure

- 1 Dans le volet **Navigateur**, cliquez sur **Stockage**.
- 2 Dans l'onglet **Mémoire persistante**, affichez les informations relatives à la banque de données PMem hôte-locale.
  - Cliquez sur **Modules** pour afficher les informations relatives aux NVDIMM qui constituent la banque de données PMem.
  - Cliquez sur **Espaces de noms** pour afficher les informations relatives aux espaces de noms sur les NVDIMM.
  - Cliquez sur **Ensembles d'entrelacement** pour voir comment les modules, ou les NVDIMM physiques, sont regroupés en ensembles d'entrelacement.

## Supprimer un espace de noms dans VMware Host Client

Dans VMware Host Client, vous pouvez supprimer des espaces de noms qui n'ont pas été créés par ESXi, mais l'ont été par un système d'exploitation précédemment installé sur l'ordinateur hôte.

### Conditions préalables

- Placez l'hôte en mode de maintenance.
- Sauvegardez le contenu de l'espace de noms dans l'éventualité où vous auriez besoin de ce contenu ultérieurement.

**Procédure**

- 1 Dans VMware Host Client, cliquez sur **Stockage**.
- 2 Sous l'onglet **Mémoire persistante**, cliquez sur **Espaces de noms**.
- 3 (Facultatif) Dans la liste des espaces de noms, consultez la colonne État pour déterminer les espaces de noms qu'ESXi utilise actuellement.

Pour libérer de l'espace, vous devez supprimer les espaces de noms dont l'état est En cours d'utilisation.

- 4 Sélectionnez un espace de noms et cliquez sur l'icône **Supprimer**.

---

**Important** La suppression d'un espace de noms libère de l'espace sur la banque de données, mais vous ne pouvez utiliser l'espace libre qu'après le redémarrage de l'hôte.

---

- 5 Cliquez sur l'icône **Redémarrer l'hôte** pour redémarrer l'hôte.

**Résultats**

L'espace de noms sélectionné est supprimé de la banque de données PMem. ESXi crée automatiquement un espace de noms qui peut être utilisé par la banque de données PMem. Le nouvel espace de noms a la même capacité, le même type et le même ID d'emplacement que l'espace de noms supprimé.

## Surveillance du stockage dans VMware Host Client

Dans VMware Host Client, vous pouvez surveiller la santé du stockage de l'hôte ESXi que vous gérez. Vous pouvez également consulter les événements et tâches associés aux différentes banques de données, adaptateurs de stockage et périphériques de stockage sur l'hôte que vous gérez.

### Surveiller les banques de données dans VMware Host Client

Dans VMware Host Client, vous pouvez surveiller la santé d'une banque de données ainsi que les événements et tâches associés à cette banque de données. À partir de vSphere 6.5 Update 1 et après l'activation du service vSAN dans vSphere Client, vous pouvez également surveiller votre environnement vSAN.

**Procédure**

- 1 Cliquez sur **Stockage** dans l'inventaire VMware Host Client.
- 2 Cliquez sur **Banques de données**.
- 3 Cliquez sur une banque de données de la liste.

La banque de données se développe dans l'inventaire VMware Host Client.

- 4 Cliquez sur **Surveiller** sous le nom de la banque de données.

- 5 (Facultatif) Cliquez sur **Événements** pour afficher les événements associés à la banque de données.
- 6 (Facultatif) Cliquez sur **vSAN** pour afficher les paramètres de configuration de l'environnement vSAN de votre hôte.
- 7 (Facultatif) Cliquez sur **Hôtes** pour afficher les hôtes qui résident sur cette banque de données.
- 8 (Facultatif) Cliquez sur **Santé** pour afficher les détails de l'état de divers paramètres, tels que **Service de performance**, **Réseau**, **Disque physique**, **Données**, **Cluster** et **Limites**.

## Surveillance de vSAN dans VMware Host Client

Vous pouvez utiliser VMware Host Client pour surveiller l'environnement vSAN de votre hôte ESXi.

### Concepts vSAN

VMware vSAN utilise une approche définie par logiciel pour créer le stockage partagé pour les machines virtuelles. Il virtualise les ressources de stockage physique local des hôtes ESXi et les transforme en pools de stockage pouvant être divisés et attribués à des machines virtuelles et à des applications en fonction de leurs conditions requises en termes de qualité de service. vSAN est implémenté directement dans l'hyperviseur ESXi.

Vous pouvez configurer vSAN pour fonctionner comme un cluster hybride ou intégralement Flash. Dans les cluster hybrides, les périphériques Flash sont utilisés pour la couche de cache et les disques magnétiques sont utilisés pour la couche de capacité de stockage. Dans les clusters intégralement Flash, des périphériques Flash sont utilisés à la fois pour le cache et la capacité.

Vous pouvez activer vSAN sur vos clusters hôtes existants et lors de la création de nouveaux clusters. vSAN agrège tous les périphériques de capacité locaux en une banque de données unique partagée par tous les hôtes du cluster vSAN. Vous pouvez développer la banque de données en ajoutant des périphériques de capacité ou des hôtes avec périphériques de capacité au cluster. vSAN fonctionne mieux lorsque tous les autres ESXi dans le cluster partagent des configurations similaires ou identiques avec tous les membres du cluster, y compris des configurations de stockage similaires ou identiques. Cela garantit l'équilibrage des composants de stockage de machine virtuelle entre tous les périphériques et hôtes du cluster. Les hôtes sans aucun périphérique local peuvent également participer et exécuter leurs machines virtuelles sur la banque de données vSAN.

Si un hôte fournit ses périphériques de stockage locaux à la banque de données vSAN, il doit fournir au moins un périphérique pour le cache Flash et au moins un périphérique pour la capacité. Les périphériques de capacité sont également appelés disques de données.

Les périphériques situés sur l'hôte contributeur forment un ou plusieurs groupes de disques. Chaque groupe de disques contient un périphérique cache Flash ou un ou plusieurs périphériques de capacité pour le stockage permanent. Chaque hôte peut être configuré pour utiliser plusieurs groupes de disques.

Pour obtenir des conseils, des informations sur la capacité et des recommandations générales sur la conception et le dimensionnement d'un cluster vSAN, reportez-vous au *Guide de dimensionnement et de conception de VMware vSAN*.

## Caractéristiques de vSAN

Cette rubrique récapitule les caractéristiques qui s'appliquent à vSAN, ses clusters et banques de données.

vSAN fournit de nombreux avantages à votre environnement.

**Tableau 6-1. Fonctionnalités vSAN**

| Fonctionnalités prises en charge                                  | Description  |
|---|--|
| Prise en charge du stockage partagé                               | vSAN prend en charge des fonctions VMware qui nécessitent un stockage partagé, telles que HA, vMotion et DRS. Par exemple, si un hôte devient surchargé, DRS peut migrer des machines virtuelles vers d'autres hôtes du cluster.   |
| Format sur disque   | Le format de fichier virtuel sur disque de vSAN fournit une prise en charge extrêmement évolutive de la gestion de snapshots et de clones par cluster vSAN. Pour plus d'informations sur le nombre de snapshots et de clones de machine virtuelle pris en charge par cluster vSAN, reportez-vous à la documentation <i>Configurations maximales</i> .  |
| Configurations intégralement Flash et hybrides                    | vSAN peut être configuré pour un cluster intégralement Flash ou hybride.   |
| Domaines de pannes  | vSAN prend en charge la configuration des domaines de pannes pour protéger les hôtes des pannes de rack ou de châssis lorsque le cluster vSAN couvre plusieurs racks ou châssis de serveurs lames dans un centre de données.   |
| service cible iSCSI   | Le service cible iSCSI vSAN permet aux hôtes et aux charges de travail physiques qui résident en dehors du cluster vSAN d'accéder à la banque de données vSAN.   |
| Cluster étendu  | vSAN prend en charge les clusters étendus couvrant deux emplacements géographiques.  |
| Prise en charge des clusters de basculement Windows Server (WSFC) | <p>vSAN 6.7 Update 3 et les versions ultérieures prennent en charge les réservations persistantes SCSI-3 (SCSI3-PR) sur un niveau de disque virtuel requis par le cluster de basculement Windows Server (WSFC) pour arbitrer un accès à un disque partagé entre des nœuds. La prise en charge de des PR SCSI-3 permet la configuration de WSFC avec une ressource de disque partagée entre des machines virtuelles en mode natif sur des banques de données vSAN.</p> <p>Actuellement, les configurations suivantes sont prises en charge :</p> <ul style="list-style-type: none"> <li>■ Jusqu'à 6 nœuds d'application par cluster.</li> <li>■ Jusqu'à 64 disques virtuels partagés par nœud.</li> </ul> <p><b>Note</b> Microsoft SQL Server 2012 ou version ultérieure s'exécutant sur Microsoft Windows Server 2012 ou version ultérieure a été qualifié sur vSAN.</p> |



Tableau 6-1. Fonctionnalités vSAN (suite)

| Fonctionnalités prises en charge                            | Description  |
|---|--|
| service de santé vSAN                                       | Le service de santé vSAN inclut des tests de contrôle de santé préconfigurés pour surveiller, dépanner, diagnostiquer la cause de problèmes de composants de cluster et identifier les risques potentiels.   |
| service de performance vSAN                                 | Le service de performance de vSAN inclut des graphiques statistiques utilisés pour surveiller l'IOPS, le débit, la latence et la congestion. Vous pouvez surveiller les performances d'un cluster, d'un hôte, d'un groupe de disques, d'un disque et de machines virtuelles vSAN.  |
| Intégration avec les fonctionnalités de stockage de vSphere | vSAN s'intègre aux fonctions de gestion de données de vSphere traditionnellement utilisées avec un stockage VMFS et NFS. Ces fonctionnalités incluent les snapshots, les clones liés et vSphere Replication.   |
| Stratégies de stockage de machine virtuelle                 | vSAN utilise des stratégies de stockage VM pour prendre en charge une approche à la gestion du stockage centrée sur les machines virtuelles.<br><br>Si vous n'attribuez pas de stratégie de stockage à la machine virtuelle lors du déploiement, la stratégie de stockage vSAN par défaut est automatiquement attribuée à la machine virtuelle.  |
| Provisionnement rapide                                      | vSAN permet le provisionnement rapide du stockage dans vCenter Server <sup>®</sup> pendant les opérations de création et de déploiement de machine virtuelle.  |
| Déduplication et compression                                | vSAN effectue une déduplication et une compression au niveau des blocs pour économiser l'espace de stockage. Lorsque vous activez la déduplication et la compression sur un cluster vSAN intégralement Flash, les données redondantes dans chaque groupe de disques sont réduites. La déduplication et la compression sont activées en tant que paramètres à l'échelle du cluster, mais elles sont appliquées au niveau du groupe de disques. Le vSAN de compression seule est appliqué sur une base par disque. |
| Chiffrement des données au repos                            | vSAN assure le chiffrement des données au repos. Les données sont chiffrées une fois que tous les autres traitements, tels que la déduplication, ont été effectués. Le chiffrement des données au repos protège les données sur les périphériques de stockage au cas où l'un d'entre eux serait supprimé du cluster.   |
| Prise en charge du SDK                                      | VMware vSAN SDK for Java est une extension de VMware vSphere Management SDK. Ce SDK comprend de la documentation, des bibliothèques et des exemples de code qui permettent aux développeurs d'automatiser l'installation, la configuration, la surveillance et le dépannage de vSAN.   |

## Surveiller vSAN dans VMware Host Client

Vous pouvez utiliser VMware Host Client pour surveiller l'environnement vSAN de votre hôte ESXi.

## Conditions préalables

Le service vSAN doit être activé dans vSphere Client avant de pouvoir afficher les écrans relatifs à vSAN pour une banque de données.

## Procédure

1 Cliquez sur **Stockage** dans l'inventaire VMware Host Client.

2 Dans l'onglet **Banques de données**, cliquez sur **Banque de données vSAN**.

La banque de données vSAN se développe dans le navigateur VMware Host Client.

3 Cliquez sur **Surveiller**.

Vous pouvez retrouver les onglets **vSAN**, **Hôte** et **Santé** dans l'interface utilisateur.

| Option       | Description  |
|--------------|--|
| <b>vSAN</b>  | <p>Affiche les configurations de l'hôte actuel. Vous pouvez modifier les paramètres pour le mode de réclamation et la déduplication. Vous pouvez également afficher les paramètres pour le :</p> <ul style="list-style-type: none"> <li>■ Chiffrement – vSAN prend en charge le chiffrement des informations pour la banque de données vSAN dans son ensemble.</li> <li>■ Service iSCSI – Service supplémentaire via le service iSCSI.</li> <li>■ Service de performance - Collecte des données sur le fonctionnement de la banque de données. Par exemple, la vitesse d'une opération de lecture ou d'écriture.</li> </ul>  |
| <b>Hôtes</b> | Affiche une liste de tous les hôtes sur le serveur vSAN avec leur adresse IP et le domaine de pannes auquel elles appartiennent.   |
| <b>Santé</b> | <p>L'onglet <b>Santé</b> contient des tests organisés en plusieurs groupes. Vous pouvez retrouver les groupes suivants :</p> <ul style="list-style-type: none"> <li>■ Service de performance</li> <li>■ Réseau</li> <li>■ Disque physique</li> <li>■ Données</li> <li>■ Cluster</li> <li>■ Limites</li> </ul> <p>Chaque groupe est étiqueté avec une icône d'état d'erreur, d'avertissement, inconnu ou sain. L'état du groupe représente l'état le plus grave obtenu au test appartenant à ce groupe. Pour afficher les tests et leurs descriptions, cliquez sur l'icône de développement dans le coin supérieur droit du groupe d'intérêt. À partir de la carte développée, vous pouvez vérifier tous les tests appartenant au groupe, le résultat de leur exécution et obtenir plus d'informations sur ce que chaque test examine sur le système.</p> |

4 Sélectionnez le paramètre vSAN que vous souhaitez surveiller.

## Modifier les paramètres d'une banque de données vSAN

Vous pouvez modifier les paramètres d'une banque de données vSAN lorsque vous devez sortir d'un état mal configuré de l'hôte actuel.

Vous pouvez modifier uniquement le **Mode de réclamation** et les paramètres de **Déduplication** d'une banque de données vSAN. Ces modifications prennent effet uniquement sur l'hôte actuel. Elles ne sont pas synchronisées avec les autres hôtes participant au cluster vSAN.

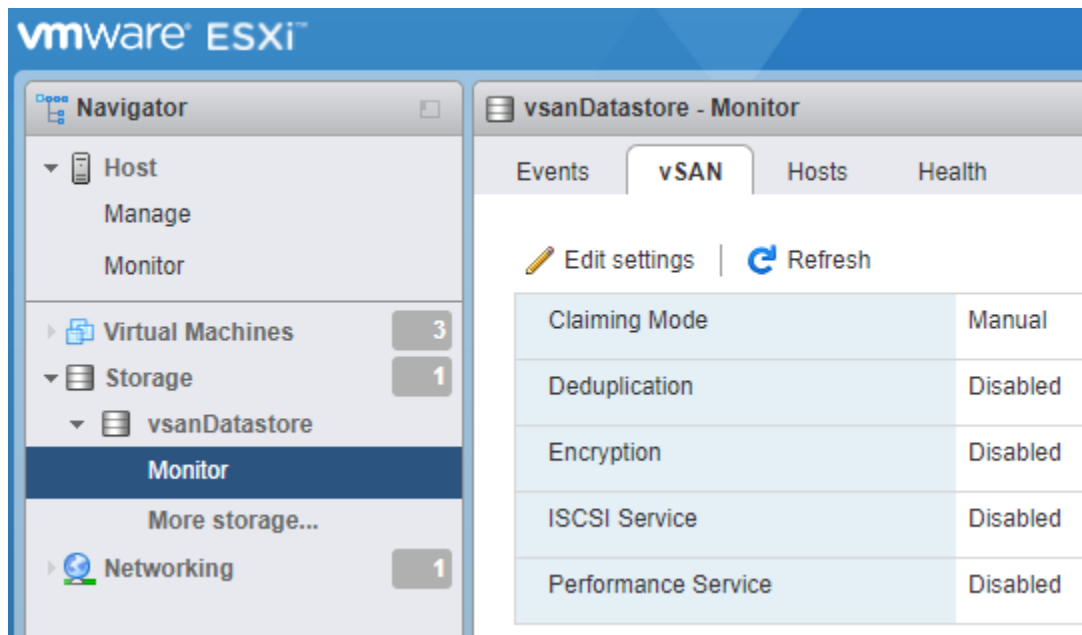
---

**Note** Utilisez ces paramètres uniquement pour le dépannage.

---

#### Procédure

- 1 Cliquez sur **Stockage** dans l'inventaire VMware Host Client.
- 2 Dans l'onglet **Banques de données**, cliquez sur une banque de données vSAN dans le tableau.
- 3 Cliquez sur **Surveiller**, puis sur l'onglet **vSAN**.



- 4 Cliquez sur **Modifier les paramètres**.  
La boîte de dialogue **Modifier les paramètres** s'ouvre.

- 5 Modifiez les paramètres. Sélectionnez **Auto** ou **Manuel** dans le **Mode de réclamation**.

| Option              | Action  |
|---------------------|---|
| Mode de réclamation | <p>a Sélectionnez <b>Auto</b> ou <b>Manuel</b> dans le <b>Mode de réclamation</b>.</p> <ul style="list-style-type: none"> <li>■ Si vous sélectionnez <b>Auto</b>, le mode de réclamation prend automatiquement tous les disques et les réclame dans un groupe ou des groupes de taille identique.</li> </ul> <hr/> <p><b>Note</b> Le mode <b>Auto</b> est obsolète. Il peut réclamer uniquement des groupes de disques hybrides qui ne sont pas compatibles avec la plupart des fonctions vSAN.</p> <hr/> <ul style="list-style-type: none"> <li>■ Si vous sélectionnez <b>Manuel</b>, vous devez organiser manuellement les disques en groupes et les récupérer à l'aide de vSphere Web Client. Par exemple, la sélection du mode de réclamation manuel est appropriée lorsque l'instance de vCenter Server n'est pas disponible.</li> </ul> |
| Déduplication       | a Sélectionnez <b>Activée</b> ou <b>Désactivée</b> pour la <b>Déduplication</b> .   |

- 6 Cliquez sur **Enregistrer**.

## Effectuer une actualisation du stockage et des opérations de réanalyse dans VMware Host Client

L'opération d'actualisation des banques de données, des périphériques de stockage et des adaptateurs de stockage met à jour les listes et les informations de stockage affichées dans VMware Host Client. Elle met à jour des informations telles que la capacité des banques de données. Lorsque vous effectuez des tâches de gestion des banques de données ou que vous modifiez la configuration SAN, il se peut que vous deviez réanalyser le stockage.

### Exécution d'une réanalyse des adaptateurs dans VMware Host Client

Lorsque vous modifiez votre configuration SAN et que ces modifications ne concernent que le stockage accessible par un adaptateur spécifique, effectuez une réanalyse pour cet adaptateur uniquement. Lorsque vous réanalysez un adaptateur, vous découvrez tous les nouveaux LUN disponibles sur cet adaptateur.

#### Procédure

- 1 Cliquez sur **Stockage** dans l'inventaire VMware Host Client et cliquez sur **Adaptateurs**.
- 2 Cliquez sur **Réanalyser**.

### Exécution d'une réanalyse de périphériques dans VMware Host Client

Lorsque vous réanalysez un périphérique, vous découvrez tous les nouveaux volumes VMFS disponibles sur le périphérique.

**Procédure**

- 1 Cliquez sur **Stockage** dans l'inventaire VMware Host Client et cliquez sur **Périphériques**.
- 2 Cliquez sur **Réanalyser**.

## Modifier le nombre de périphériques de stockage analysés dans VMware Host Client

La plage d'ID de LUN analysés pour un hôte ESXi peut être comprise entre 0 et 16 383. ESXi ignore les ID de LUN supérieurs à 16 383. Le paramètre `Disk.MaxLUN` configurable détermine la plage d'ID de LUN analysée. Ce paramètre a une valeur par défaut de 1 024.

Le paramètre `Disk.MaxLUN` détermine également le nombre de LUN que le code d'analyse SCSI tente de détecter en utilisant des commandes INQUIRY individuelles si la cible SCSI ne prend pas en charge la détection directe en utilisant REPORT\_LUNS.

Vous pouvez modifier le paramètre `Disk.MaxLUN` en fonction de vos besoins. Par exemple, si votre environnement comporte un plus petit nombre de périphériques de stockage avec des ID de LUN compris entre 1 et 100, définissez la valeur sur 101. Cela permet d'améliorer la vitesse de découverte des périphériques sur les cibles ne prenant pas en charge REPORT\_LUNS. Diminuer cette valeur peut raccourcir la durée de réanalyse et d'amorçage. Cependant, la durée de réanalyse des périphériques de stockage peut également dépendre d'autres facteurs, notamment du type de système de stockage et de la charge sur le système de stockage.

Dans d'autres cas, il peut être nécessaire d'augmenter la valeur si votre environnement utilise des ID de LUN supérieurs à 1023.

**Procédure**

- 1 Cliquez sur **Gérer** dans l'inventaire VMware Host Client et cliquez sur **Paramètres avancés**.
- 2 Faites défiler jusqu'à `Disk.MaxLUN`.
- 3 Cliquez avec le bouton droit sur `Disk.MaxLUN`, puis cliquez sur **Modifier l'option**.
- 4 Entrez une nouvelle valeur et cliquez sur **Enregistrer**.

Le code d'analyse SCSI n'analyse pas les LUN dont les ID sont supérieurs ou égaux à la valeur que vous entrez.

Par exemple, pour détecter les ID des LUN 0 à 100, affectez à `Disk.MaxLUN` la valeur 101.

# Mise en réseau dans VMware Host Client

# 7

Lorsque vous vous connectez à un hôte ESXi avec VMware Host Client, vous pouvez afficher et configurer les commutateurs vSphere standard, les groupes de ports, les cartes réseau VMkernel, et les piles TCP/IP.

Ce chapitre contient les rubriques suivantes :

- [Gérer les groupes de ports dans VMware Host Client](#)
- [Gérer des commutateurs virtuels dans VMware Host Client](#)
- [Gérer les adaptateurs réseau physiques dans VMware Host Client](#)
- [Gérer des adaptateurs réseau VMkernel dans VMware Host Client](#)
- [Afficher la configuration des piles TCP/IP sur un hôte dans VMware Host Client](#)
- [Modifier la configuration d'une pile TCP/IP sur un hôte dans VMware Host Client](#)
- [Configurer le pare-feu ESXi dans VMware Host Client](#)
- [Surveiller des événements et tâches de mise en réseau dans VMware Host Client](#)

## Gérer les groupes de ports dans VMware Host Client

Vous pouvez gérer les paramètres des groupes de ports pour configurer la gestion du trafic, améliorer la sécurité de la mise en réseau et améliorer les performances. À l'aide de VMware Host Client, vous pouvez ajouter et supprimer des groupes de ports. Vous pouvez également examiner les informations du groupe de ports et modifier les paramètres du groupe de ports, tels que l'association de cartes réseau et le paramétrage du trafic.

## Afficher les informations sur les groupes de ports dans VMware Host Client

Dans VMware Host Client, vous pouvez afficher des informations sur la configuration des groupes de ports, les informations réseau, la topologie des commutateurs virtuels, la stratégie d'association de cartes réseau, la stratégie de déchargement et la stratégie de sécurité.

### Procédure

- 1 Cliquez sur **Mise en réseau** dans l'inventaire VMware Host Client et cliquez sur **Groupes de ports**.

- 2 Cliquez sur un élément de la liste des groupes de ports disponibles.

Les informations sur le réseau, la topologie des commutateurs virtuels, la stratégie d'association de cartes réseau, la stratégie de déchargement et la stratégie de sécurité apparaissent.

## Ajouter un groupe de ports de commutateur virtuel dans VMware Host Client

Vous pouvez ajouter un groupe de ports à un commutateur virtuel dans VMware Host Client. Les groupes de ports fournissent une mise en réseau pour les machines virtuelles.

### Procédure

- 1 Cliquez avec le bouton droit sur **Mise en réseau** dans l'inventaire VMware Host Client et cliquez sur **Ajouter un groupe de ports** dans le menu contextuel.
- 2 Entrez un nom pour le nouveau groupe de ports.
- 3 Définissez l'ID VLAN pour configurer le traitement VLAN dans le groupe de ports.

L'ID VLAN reflète également le mode de balisage VLAN dans le groupe de ports.

| Mode de balisage VLAN                 | ID VLAN     | Description   |
|---------------------------------------|-------------|---|
| Balisage de commutateur externe (EST) | 0           | Le commutateur virtuel ne transmet pas le trafic associé à un VLAN.   |
| Balisage de commutateur virtuel (VST) | De 1 à 4094 | Le commutateur virtuel marque le trafic avec la balise entrée.  |
| Balisage d'invité virtuel (VGT)       | 4095        | Les machines virtuelles gèrent des VLAN. Le commutateur virtuel autorise le trafic provenant de n'importe quel réseau VLAN. |

- 4 Sélectionnez un commutateur virtuel dans le menu déroulant.
- 5 Développez **Sécurité** et sélectionnez les options que vous souhaitez activer pour le mode promiscuité, les modifications d'adresses MAC et les transmissions forgées.
- 6 Cliquez sur **Ajouter**.  
Votre groupe de ports est créé.
- 7 (Facultatif) Cliquez sur **Actualiser** pour afficher le nouveau groupe de ports dans la liste.

## Modifier les paramètres des groupes de ports dans VMware Host Client

Pour améliorer la sécurité et les performances de la mise en réseau dans VMware Host Client, vous pouvez modifier divers paramètres de groupe de ports, tels que le nom du groupe de ports, l'ID VLAN et le commutateur virtuel. Vous pouvez également configurer la sécurité, l'association de cartes réseau et les composants de la formation du trafic.

## Procédure

- 1 Cliquez sur **Mise en réseau** dans l'inventaire VMware Host Client et cliquez sur **Groupes de ports**.
- 2 Cliquez avec le bouton droit sur le groupe de ports de la liste que vous voulez modifier, puis sélectionnez **Modifier les paramètres**.
- 3 (Facultatif) Entrez un nouveau nom de groupe de ports.
- 4 (Facultatif) Entrez une nouvelle valeur pour l'ID VLAN.

L'ID VLAN reflète le mode de balisage VLAN dans le groupe de ports.

| Mode de balisage VLAN                 | ID VLAN     | Description   |
|---------------------------------------|-------------|---|
| Balisage de commutateur externe (EST) | 0           | Le commutateur virtuel ne transmet pas le trafic associé à un VLAN.   |
| Balisage de commutateur virtuel (VST) | De 1 à 4094 | Le commutateur virtuel marque le trafic avec la balise entrée.  |
| Balisage d'invité virtuel (VGT)       | 4095        | Les machines virtuelles gèrent des VLAN. Le commutateur virtuel autorise le trafic provenant de n'importe quel réseau VLAN. |

- 5 (Facultatif) Sélectionnez un commutateur virtuel dans le menu déroulant.



- 6 (Facultatif) Développez **Sécurité** et sélectionnez de rejeter ou d'accepter les exceptions de la stratégie de sécurité, ou d'en hériter de vSwitch.

| Option                      | Description   |
|-----------------------------|---|
| Mode promiscuité            | <ul style="list-style-type: none"> <li>■ <b>Rejeter.</b> Une carte invitée en mode promiscuité n'a aucun effet sur la réception des trames qu'elle reçoit.</li> <li>■ <b>Accepter.</b> L'activation du mode promiscuité sur un adaptateur invité permet de détecter toutes les trames transmises à vSphere Distributed Switch qui sont autorisées par la stratégie VLAN pour le groupe de ports auquel l'adaptateur est connecté.</li> <li>■ <b>Hériter de vSwitch.</b> L'activation du mode promiscuité sur un adaptateur invité permet à ce dernier d'hériter de la configuration du commutateur virtuel associé.</li> </ul>  |
| Modifications d'adresse MAC | <ul style="list-style-type: none"> <li>■ <b>Rejeter.</b> Si vous définissez <b>Modifications d'adresse MAC</b> sur <b>Rejeter</b> et que le système d'exploitation invité remplace l'adresse MAC de l'adaptateur par une autre ne figurant pas dans le fichier de configuration <code>.vmtx</code>, toutes les trames entrantes sont abandonnées.<br/><br/>Si le système d'exploitation invité remplace de nouveau l'adresse MAC par celle figurant dans le fichier de configuration <code>.vmtx</code>, les trames entrantes sont retransmises.</li> <li>■ <b>Accepter.</b> La modification de l'adresse MAC depuis le système d'exploitation invité a l'effet prévu : les trames destinées à la nouvelle adresse MAC sont reçues.</li> <li>■ <b>Hériter de vSwitch.</b> Si vous définissez <b>Modifications d'adresse MAC</b> sur <b>Hériter de vSwitch</b>, l'adresse MAC est remplacée par l'une des adresses des machines virtuelles associées.</li> </ul> |
| Transmissions forgées       | <ul style="list-style-type: none"> <li>■ <b>Rejeter.</b> Toutes les trames sortantes dont l'adresse MAC source est différente de celle définie sur l'adaptateur sont abandonnées.</li> <li>■ <b>Accepter.</b> Aucun filtrage n'est exécuté et toutes les trames sortantes sont transmises.</li> <li>■ <b>Hériter de vSwitch.</b> La configuration des trames sortantes est héritée du commutateur virtuel associé.</li> </ul>   |

## 7 (Facultatif) Développez **Association de cartes réseau** et configurez les composants suivants.

| Option                                    | Description  |
|---|--|
| <b>Équilibrage de charge</b>              | <p>Spécifiez comment choisir une liaison montante.</p> <ul style="list-style-type: none"> <li>■ <b>Hériter de vSwitch.</b> Choisissez la liaison montante qui est sélectionnée pour le commutateur virtuel associé.</li> <li>■ <b>Route basée sur le hachage IP.</b> 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.</li> <li>■ <b>Route basée sur le hachage MAC source.</b> Choisissez une liaison montante en fonction d'un hachage de l'Ethernet source.</li> <li>■ <b>Route basée sur l'ID du port d'origine</b> Choisissez une liaison montante basée sur l'ID du port d'origine.</li> <li>■ <b>Utiliser la commande de basculement explicite.</b> Utilisez toujours la liaison montante d'ordre supérieur dans la liste des adaptateurs actifs qui transmettent les critères de détection du basculement.</li> </ul> <p><b>Note</b> L'association basée sur IP exige que le commutateur physique soit configuré avec EtherChannel. Pour toutes les autres options, EtherChannel doit être désactivé.</p> |
| <b>Détection de basculement de réseau</b> | <p>Spécifiez la méthode pour l'utiliser pour la détection de basculement.</p> <ul style="list-style-type: none"> <li>■</li> <li>■ <b>Hériter de vSwitch.</b> Hérite la configuration respective du commutateur virtuel associé.</li> <li>■ <b>État de lien seulement.</b> Repose uniquement sur l'état du lien fourni par l'adaptateur réseau. Cette option détecte les pannes, 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.</li> <li>■ <b>Balise seulement.</b> Envoie et détecte des sondes d'incident sur toutes les cartes réseau de l'association et utilise cette information, reliée à l'état du lien, pour déterminer les défaillances de liens. Cela détecte plusieurs des échecs qui ne sont pas détectés par l'état du lien seulement.</li> </ul> <p><b>Note</b> Ne choisissez pas le sondage de balise avec l'équilibrage de charge avec hachage IP.</p>                                     |

| Option                           | Description   |
|----------------------------------|---|
| <b>Notifier les commutateurs</b> | <p>Sélectionnez <b>Oui</b>, <b>Non</b> ou <b>Hériter de vSwitch</b> pour notifier les commutateurs en cas de basculement.</p> <p>Si vous sélectionnez <b>Oui</b>, chaque fois qu'une carte réseau virtuelle est connectée au commutateur distribué ou que le trafic de cette carte est acheminé sur une carte réseau physique différente dans l'association suite à un basculement, une notification est envoyée sur le réseau pour mettre à jour les tables de recherche des commutateurs physiques. Dans presque tous les cas, ce processus est utilisé de préférence pour obtenir la plus basse latence dans les occurrences de basculement et les migrations avec vMotion.</p> <hr/> <p><b>Note</b> N'utilisez pas cette option quand les machines virtuelles utilisant le groupe de ports utilisent l'équilibrage de charge réseau Microsoft dans le mode monodiffusion. Ce problème n'existe pas lorsque NLB fonctionne en mode multidiffusion.</p>                                   |
| <b>Retour arrière</b>            | <p>Sélectionnez <b>Oui</b>, <b>Non</b> ou <b>Hériter de vSwitch</b> pour désactiver ou activer le basculement.</p> <p>Cette option détermine le mode de retour en activité d'un adaptateur physique lors de la récupération après échec. Si le basculement est défini sur <b>Oui</b>, l'adaptateur revient en service actif immédiatement après la récupération, en déplaçant l'adaptateur en veille qui a occupé son emplacement le cas échéant. Si le retour arrière est défini sur <b>Non</b>, un adaptateur défectueuse est laissé inactive, même après la récupération, jusqu'à ce qu'une autre carte actuellement active échoue, exigeant son remplacement.</p>   |
| <b>ordre de basculement</b>      | <p>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 :</p> <ul style="list-style-type: none"> <li>■ <b>Liaisons montantes actives.</b> Continuez à utiliser la liaison montante si la connectivité de l'adaptateur réseau est disponible et en activité.</li> <li>■ <b>Liaisons montantes en veille.</b> Utilisez cette liaison montante si la connectivité de l'un des adaptateurs actif est indisponible.</li> </ul> <hr/> <p><b>Note</b> En utilisant l'équilibrage de charge pas hachage IP, ne configurez pas les liaisons montantes en veille. Vous ne pouvez pas configurer l'ordre de basculement si des composants du groupe de ports sont configurés pour hériter la configuration du commutateur virtuel associé.</p> |

- 8 (Facultatif) Pour configurer la formation du trafic, développez **Formation du trafic**, cliquez sur **Activé**, puis spécifiez les paramètres suivants.

| Option                         | Description  |
|--------------------------------|--|
| <b>Bande passante moyenne</b>  | Définit le nombre de bits moyen par seconde à autoriser sur un port dans le temps (charge moyenne autorisée).  |
| <b>Bande passante maximale</b> | Nombre maximal de bits par seconde à autoriser sur un port quand il reçoit/ envoie une rafale de trafic. Il s'agit de la bande passante maximale utilisée par un port lorsqu'il utilise son bonus de rafale.   |
| <b>Taille de rafale</b>        | 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 <b>Bande passante moyenne</b> , il peut être autorisé à transmettre temporairement des données à une vitesse plus élevée si un bonus de rafale est disponible. Ce paramètre représente le nombre maximal d'octets qui peuvent être accumulés dans le bonus de rafale et donc transférés à une vitesse plus élevée. |

La stratégie de formation du trafic est appliquée au trafic de chaque adaptateur réseau virtuel attaché au commutateur virtuel.

- 9 Cliquez sur **Enregistrer** pour appliquer vos modifications.

## Supprimer un groupe de ports de commutateur virtuel dans VMware Host Client

Vous pouvez supprimer des groupes de ports de commutateurs virtuels si vous n'avez plus besoin d'utiliser les réseaux étiquetés associés.

### Conditions préalables

Assurez-vous qu'aucun adaptateur réseau VMkernel et qu'aucune machine virtuelle sous tension n'est connectée au groupe de ports à supprimer.

### Procédure

- 1 Cliquez sur **Mise en réseau** dans l'inventaire VMware Host Client et cliquez sur l'onglet **Groupes de ports**.
- 2 Cliquez avec le bouton droit sur le groupe de ports que vous souhaitez supprimer et sélectionnez **Supprimer** dans le menu contextuel.
- 3 Pour supprimer le groupe de ports, cliquez sur **Supprimer**.
- 4 (Facultatif) Cliquez sur **Actualiser** pour vérifier que vous avez supprimé le groupe de ports.

## Gérer des commutateurs virtuels dans VMware Host Client

Dans VMware Host Client, vous pouvez configurer divers paramètres de commutateur virtuel, tels que la découverte de liaison, l'association de cartes réseau et la formation du trafic.

## Afficher les informations sur les commutateurs virtuels dans VMware Host Client

Dans VMware Host Client, vous pouvez afficher les informations sur les commutateurs virtuels, comme des informations sur la configuration et le réseau, la topologie des commutateurs virtuels, etc.

### Procédure

- 1 Cliquez sur **Mise en réseau** dans l'inventaire VMware Host Client et cliquez sur **Commutateurs virtuels**.
- 2 Cliquez sur un commutateur de la liste des commutateurs virtuels disponibles.

Des informations sur la configuration des commutateurs virtuels, sur le réseau, et sur la topologie des commutateurs virtuels apparaissent.

## Ajouter un commutateur virtuel standard dans VMware Host Client

Dans VMware Host Client, vous pouvez ajouter un commutateur virtuel standard pour fournir une connectivité réseau à l'hôte que vous gérez et aux machines virtuelles sur cet hôte, ainsi que pour gérer le trafic VMkernel. Selon le type de connexion que vous souhaitez créer, vous pouvez créer un commutateur vSphere standard avec un adaptateur VMkernel, connecter un adaptateur réseau physique existant au nouveau commutateur ou créer le commutateur avec un groupe de ports de machine virtuelle.

### Procédure

- 1 Cliquez avec le bouton droit sur **Mise en réseau** dans l'inventaire VMware Host Client et cliquez sur **Ajouter vSwitch standard** depuis le menu contextuel.
- 2 (Facultatif) Cliquez sur **Ajouter une liaison montante** pour ajouter une nouvelle liaison montante physique à un commutateur virtuel.
- 3 Entrez un nom pour le commutateur virtuel et cliquez sur **Créer un commutateur virtuel**.
- 4 Sélectionnez une liaison montante pour le commutateur virtuel.
- 5 Développez **Découverte de liaison** et sélectionnez une option pour le mode commutateur virtuel.

| Opération | Description  |
|-----------|--|
| Écouter   | ESXi détecte et affiche les informations sur le port physique de commutateur associé, mais l'administrateur du commutateur n'a pas accès aux informations sur le commutateur vSphere standard. |
| Annoncer  | ESXi met les informations sur le commutateur vSphere standard à disposition de l'administrateur du commutateur, mais ne détecte ni n'affiche aucune information sur le commutateur physique.   |

| Opération | Description   |
|-----------|---|
| Les deux  | ESXi détecte et affiche les informations sur le commutateur physique associé et met les informations sur le commutateur vSphere standard à la disposition de l'administrateur du commutateur.     |
| Aucun     | ESXi ne détecte ni n'affiche les informations sur le port physique de commutateur associé, et l'administrateur du commutateur n'a pas accès aux informations sur le commutateur vSphere standard. |

- 6 Dans la section Protocole, sélectionnez **Cisco Discovery Protocol** dans le menu déroulant.
- 7 Développez **Sécurité**, et acceptez ou refusez le mode promiscuité, les modifications d'adresses MAC et les transmissions forgées des machines virtuelles reliées au commutateur standard.

| Option                      | Description   |
|-----------------------------|---|
| Mode promiscuité            | <ul style="list-style-type: none"> <li>■ <b>Rejeter.</b> L'adaptateur réseau de la machine virtuelle ne reçoit que les trames adressées à la machine virtuelle.</li> <li>■ <b>Accepter.</b> Le commutateur virtuel transmet toutes les trames à la machine virtuelle conformément à la stratégie VLAN active du port auquel l'adaptateur réseau de la machine virtuelle est connecté.</li> </ul> <p><b>Note</b> Le mode promiscuité est un mode de fonctionnement non sécurisé. Les pare-feu, scanners de ports, systèmes de détection d'intrusion, doivent s'exécuter en mode promiscuité.</p>   |
| Modifications d'adresse MAC | <ul style="list-style-type: none"> <li>■ <b>Rejeter.</b> Si le système d'exploitation invité remplace l'adresse MAC effective de la machine virtuelle par une valeur différente de l'adresse MAC de l'adaptateur réseau de la machine virtuelle (définie dans le fichier de configuration <code>.vmx</code>), le commutateur rejette toutes les trames entrantes de l'adaptateur.</li> </ul> <p>Si le système d'exploitation invité remplace à nouveau l'adresse MAC effective de la machine virtuelle par l'adresse MAC de l'adaptateur réseau de la machine virtuelle, la machine virtuelle reçoit de nouveau les trames.</p> <ul style="list-style-type: none"> <li>■ <b>Accepter.</b> Si le système d'exploitation invité remplace l'adresse MAC effective de la machine virtuelle par une valeur différente de l'adresse MAC de l'adaptateur réseau de la machine virtuelle, le commutateur autorise la transmission des trames vers la nouvelle adresse.</li> </ul> |
| Transmissions forgées       | <ul style="list-style-type: none"> <li>■ <b>Rejeter.</b> Le commutateur ignore toutes les trames sortantes provenant d'un adaptateur de machine virtuelle dont l'adresse MAC source est différente de celle qui figure dans le fichier de configuration <code>.vmx</code>.</li> <li>■ <b>Accepter.</b> Le commutateur n'effectue pas de filtrage et autorise toutes les trames sortantes.</li> </ul>  |

- 8 Cliquez sur **Add**.

## Supprimer un commutateur virtuel dans VMware Host Client

Vous pouvez supprimer le commutateur virtuel standard si vous n'en avez plus besoin.

**Procédure**

- 1 Cliquez sur **Mise en réseau** dans l'inventaire VMware Host Client et cliquez sur l'onglet **Commutateurs virtuels**.
- 2 Cliquez avec le bouton droit sur l'adaptateur virtuel que vous voulez supprimer de la liste, puis cliquez sur **Supprimer**.
- 3 Cliquez sur **Yes**.

## Ajouter une liaison montante physique à un commutateur virtuel dans VMware Host Client

Vous pouvez connecter plusieurs adaptateurs à un seul commutateur vSphere standard pour fournir l'association de cartes réseau. L'association peut partager du trafic et fournir un basculement.

**Procédure**

- 1 Cliquez sur **Mise en réseau** dans l'inventaire VMware Host Client et cliquez sur **Commutateurs virtuels**.
- 2 Cliquez sur un commutateur virtuel dans la liste et cliquez sur **Ajouter une liaison montante**.
- 3 Sélectionnez une carte réseau physique parmi les options disponibles.
- 4 Cliquez sur **Enregistrer**.

## Modifier les paramètres des commutateurs virtuels dans VMware Host Client

Dans VMware Host Client, vous pouvez modifier les paramètres de commutateur virtuel, tels que les liaisons montantes de commutateur virtuel.

**Procédure**

- 1 Cliquez sur **Mise en réseau** dans l'inventaire VMware Host Client et cliquez sur **Commutateurs virtuels**.
- 2 Cliquez avec le bouton droit sur le commutateur virtuel que vous voulez modifier, puis cliquez sur **Modifier les paramètres**.
- 3 (Facultatif) Cliquez sur **Ajouter une liaison montante** pour ajouter une nouvelle liaison montante physique au commutateur virtuel.
- 4 Modifiez l'unité de transmission maximale (MTU, maximum transmission unit).  
Le paramètre MTU améliore l'efficacité de la mise en réseau en augmentant la quantité de données de charge utile transmise dans un paquet, c'est-à-dire en activant les trames Jumbo.
- 5 (Facultatif) Cliquez sur l'icône **Supprimer** (🗑️) pour supprimer l'ancienne liaison montante du commutateur virtuel.

- 6 Développez **Découverte de liaison** et sélectionnez une option pour le mode commutateur virtuel.

| Opération       | Description   |
|-----------------|---|
| <b>Écouter</b>  | ESXi détecte et affiche les informations sur le port physique de commutateur associé, mais l'administrateur du commutateur n'a pas accès aux informations sur le commutateur vSphere standard.    |
| <b>Annoncer</b> | ESXi met les informations sur le commutateur vSphere standard à disposition de l'administrateur du commutateur, mais ne détecte ni n'affiche aucune information sur le commutateur physique.      |
| <b>Les deux</b> | ESXi détecte et affiche les informations sur le commutateur physique associé et met les informations sur le commutateur vSphere standard à la disposition de l'administrateur du commutateur.     |
| <b>None</b>     | ESXi ne détecte ni n'affiche les informations sur le port physique de commutateur associé, et l'administrateur du commutateur n'a pas accès aux informations sur le commutateur vSphere standard. |

- 7 Dans la section Protocole, sélectionnez **Cisco Discovery Protocol** dans le menu déroulant.



- 8 Développez **Sécurité**, et acceptez ou refusez le mode promiscuité, les modifications d'adresses MAC et les transmissions forgées des machines virtuelles reliées au commutateur standard.

| Option                      | Description   |
|-----------------------------|---|
| Mode promiscuité            | <ul style="list-style-type: none"> <li>■ <b>Rejeter.</b> L'adaptateur réseau de la machine virtuelle ne reçoit que les trames adressées à la machine virtuelle.</li> <li>■ <b>Accepter.</b> Le commutateur virtuel transmet toutes les trames à la machine virtuelle conformément à la stratégie VLAN active du port auquel l'adaptateur réseau de la machine virtuelle est connecté.</li> </ul> <p><b>Note</b> Le mode promiscuité est un mode de fonctionnement non sécurisé. Les pare-feu, scanners de ports, systèmes de détection d'intrusion, doivent s'exécuter en mode promiscuité.</p>   |
| Modifications d'adresse MAC | <ul style="list-style-type: none"> <li>■ <b>Rejeter.</b> Si le système d'exploitation invité remplace l'adresse MAC effective de la machine virtuelle par une valeur différente de l'adresse MAC de l'adaptateur réseau de la machine virtuelle (définie dans le fichier de configuration <code>.vmx</code>), le commutateur rejette toutes les trames entrantes de l'adaptateur.</li> </ul> <p>Si le système d'exploitation invité remplace à nouveau l'adresse MAC effective de la machine virtuelle par l'adresse MAC de l'adaptateur réseau de la machine virtuelle, la machine virtuelle reçoit de nouveau les trames.</p> <ul style="list-style-type: none"> <li>■ <b>Accepter.</b> Si le système d'exploitation invité remplace l'adresse MAC effective de la machine virtuelle par une valeur différente de l'adresse MAC de l'adaptateur réseau de la machine virtuelle, le commutateur autorise la transmission des trames vers la nouvelle adresse.</li> </ul> |
| Transmissions forgées       | <ul style="list-style-type: none"> <li>■ <b>Rejeter.</b> Le commutateur ignore toutes les trames sortantes provenant d'un adaptateur de machine virtuelle dont l'adresse MAC source est différente de celle qui figure dans le fichier de configuration <code>.vmx</code>.</li> <li>■ <b>Accepter.</b> Le commutateur n'effectue pas de filtrage et autorise toutes les trames sortantes.</li> </ul>  |

## 9 (Facultatif) Développez **Association de cartes réseau** et configurez les composants suivants.

| Option                             | Description  |
|------------------------------------|--|
| Équilibrage de charge              | <p>Spécifiez comment choisir une liaison montante.</p> <ul style="list-style-type: none"> <li>■ <b>Route basée sur le hachage IP.</b> 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.</li> <li>■ <b>Route basée sur le hachage MAC source.</b> Choisissez une liaison montante en fonction d'un hachage de l'Ethernet source.</li> <li>■ <b>Route basée sur l'ID du port d'origine</b> Choisissez une liaison montante basée sur l'ID du port d'origine.</li> <li>■ <b>Utiliser la commande de basculement explicite.</b> Toujours utiliser la liaison montante d'ordre supérieur dans la liste des adaptateurs actifs qui vérifient les critères de détection du basculement.</li> </ul> <p><b>Note</b> L'association basée sur IP exige que le commutateur physique soit configuré avec EtherChannel. Pour toutes les autres options, EtherChannel doit être désactivé.</p>   |
| Détection de basculement de réseau | <p>Spécifiez la méthode pour l'utiliser pour la détection de basculement.</p> <ul style="list-style-type: none"> <li>■ <b>État de lien seulement.</b> Repose uniquement sur l'état du lien fourni par l'adaptateur réseau. Cette option détecte les pannes, 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.</li> <li>■ <b>Balise seulement.</b> Envoie et détecte des sondes d'incident 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.</li> </ul> <p><b>Note</b> Ne choisissez pas le sondage de balise avec l'équilibrage de charge avec hachage IP.</p> |
| Notifier les commutateurs          | <p>Sélectionnez <b>Oui</b>, <b>Non</b> ou <b>Hériter de vSwitch</b> pour notifier les commutateurs en cas de basculement.</p> <p>Si vous sélectionnez <b>Oui</b>, chaque fois qu'une carte réseau virtuelle est connectée au commutateur distribué ou que le trafic de cette carte est acheminé sur une carte réseau physique différente dans l'association suite à un basculement, une notification est envoyée sur le réseau pour mettre à jour les tables de recherche des 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.</p> <p><b>Note</b> N'utilisez pas cette option quand les machines virtuelles utilisant le groupe de ports utilisent l'équilibrage de charge réseau Microsoft dans le mode monodiffusion. Ce problème n'existe pas lorsque NLB fonctionne en mode multidiffusion.</p>  |

| Option                      | Description  |
|-----------------------------|--|
| <b>Retour arrière</b>       | <p>Sélectionnez <b>Oui</b>, <b>Non</b> ou <b>Hériter de vSwitch</b> pour désactiver ou activer le basculement.</p> <p>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 <b>Oui</b>, 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 <b>Non</b>, un adaptateur défectueuse est laissé inactive, même après la récupération, jusqu'à ce qu'une autre carte actuellement active échoue, exigeant son remplacement.</p>   |
| <b>ordre de basculement</b> | <p>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 :</p> <ul style="list-style-type: none"> <li>■ <b>Liaisons montantes actives.</b> Continuez à utiliser la liaison montante si la connectivité de l'adaptateur réseau est disponible et en activité.</li> <li>■ <b>Liaisons montantes en veille.</b> Utilisez cette liaison montante si la connectivité de l'un des adaptateurs actif est indisponible.</li> </ul> <p><b>Note</b> En utilisant l'équilibrage de charge pas hachage IP, ne configurez pas les liaisons montantes de réserve.</p> |

- 10 (Facultatif) Pour configurer la formation du trafic, développez **Formation du trafic**, cliquez sur **Activé**, puis spécifiez les paramètres suivants.

| Option                         | Description  |
|--------------------------------|--|
| <b>Bande passante moyenne</b>  | Définit le nombre de bits moyen par seconde à autoriser sur un port dans le temps (charge moyenne autorisée).  |
| <b>Bande passante maximale</b> | 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.  |
| <b>Taille de rafale</b>        | 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 <b>Bande passante moyenne</b> , il peut être autorisé à transmettre temporairement des données à une vitesse plus élevée si un bonus de rafale est disponible. Ce paramètre s'ajoute au nombre d'octets qui peuvent être cumulés dans le bonus de rafale, puis transférés à une vitesse plus élevée. |

La stratégie de formation du trafic est appliquée au trafic de chaque adaptateur réseau virtuel attaché au commutateur virtuel.

- 11 Cliquez sur **Enregistrer**.

## Gérer les adaptateurs réseau physiques dans VMware Host Client

Attribuez un adaptateur physique à un commutateur standard pour fournir une connectivité aux machines virtuelles et aux adaptateurs VMkernel de l'hôte que vous gérez.

### Afficher les informations sur les cartes réseau physiques dans VMware Host Client

Dans VMware Host Client, vous pouvez afficher différentes informations sur la configuration et les paramètres des cartes réseau physiques (NIC).

#### Procédure

- 1 Cliquez sur **Mise en réseau** dans l'inventaire VMware Host Client et cliquez sur **Cartes réseau physiques**.
- 2 Cliquez sur la carte réseau au sujet de laquelle vous souhaitez obtenir des informations.

### Modifier les cartes réseau physiques dans VMware Host Client

Vous pouvez modifier la vitesse des cartes réseau physiques avec VMware Host Client.

#### Procédure

- 1 Cliquez sur **Mise en réseau** dans l'inventaire VMware Host Client et cliquez sur **Cartes réseau physiques**.
- 2 Sélectionnez la carte réseau que vous souhaitez modifier dans le tableau.
- 3 Cliquez sur **Modifier les paramètres** et sélectionnez une option à partir du menu déroulant.
- 4 Cliquez sur **Enregistrer**.

## Gérer des adaptateurs réseau VMkernel dans VMware Host Client

Dans VMware Host Client, vous pouvez ajouter et supprimer des adaptateurs réseau VMkernel (NIC), et afficher et modifier les paramètres des adaptateurs réseau VMkernel.

### Afficher les informations sur l'adaptateur réseau VMkernel dans VMware Host Client

Dans VMware Host Client, vous pouvez afficher les informations sur les adaptateurs réseau VMkernel (NIC), comme la configuration TCP/IP, les informations sur le réseau, la topologie des commutateurs virtuels, etc.

## Procédure

- 1 Cliquez sur **Mise en réseau** dans l'inventaire VMware Host Client et cliquez sur **Cartes réseau VMkernel**.
- 2 Cliquez sur une carte réseau dans la liste pour afficher les informations sur la configuration et la topologie.

## Ajouter un adaptateur réseau VMkernel dans VMware Host Client

Vous pouvez ajouter une carte réseau (NIC) VMkernel sur un commutateur VMware vSphere® Standard Edition™ pour assurer la connectivité réseau pour les hôtes. La carte réseau VMkernel gère également le trafic système pour le commutateur VMware vSphere® vMotion®, le stockage IP, Fault Tolerance, la journalisation, vSAN, etc.

## Procédure

- 1 Cliquez avec le bouton droit sur **Mise en réseau** dans l'inventaire VMware Host Client et cliquez sur **Ajouter une carte réseau VMkernel**.
- 2 Dans la boîte de dialogue **Ajouter une carte réseau VMkernel**, configurez les paramètres de l'adaptateur VMkernel.

| Option                            | Description  |
|-----------------------------------|--|
| Étiquette Nouveau groupe de ports | L'ajout d'une carte réseau VMkernel ajoute également un groupe de ports. Spécifiez un nom pour ce groupe de ports.                               |
| ID VLAN                           | Entrez un ID VLAN pour identifier le VLAN que le trafic réseau de l'adaptateur VMkernel utilisera.   |
| Version IP                        | Sélectionnez IPv4, IPv6 ou les deux.<br><br><b>Note</b> L'option IPv6 n'apparaît pas sur les hôtes sur lesquels l'option IPv6 n'est pas activée. |

- 3 Sélectionnez un commutateur virtuel dans le menu déroulant.
- 4 (Facultatif) Développez la section des paramètres IPv4 pour sélectionner une option permettant d'obtenir des adresses IP.

| Option  | Description  |
|---|--|
| Utilisez DHCP pour obtenir les paramètres IP. | Les paramètres IP sont obtenus automatiquement. Un serveur DHCP doit être présent sur le réseau.   |
| Utiliser des paramètres IP statiques          | Entrez l'adresse IPv4 et un masque de sous-réseau pour l'adaptateur VMkernel.<br><br>Les adresses de la passerelle par défaut VMkernel et du serveur DNS pour IPv4 proviennent de la pile TCP/IP sélectionnée. |

- 5 (Facultatif) Développez la section des paramètres IPv6 pour sélectionner une option permettant d'obtenir des adresses IPv6.

| Option                    | Description   |
|---------------------------|---|
| DHCPv6                    | Utilisez DHCP pour obtenir les adresses IPv6. Un serveur DHCPv6 doit être présent sur le réseau.  |
| Configuration automatique | Utilisez l'annonce de routage pour obtenir les adresses IPv6.   |
| Adresses IPv6 statiques   | a Cliquez sur <b>Ajouter une adresse</b> pour ajouter une nouvelle adresse IPv6.<br>b Entrez l'adresse IPv6 et la longueur du préfixe de sous-réseau. |

- 6 Sélectionnez une pile TCP/IP dans le menu déroulant.

Une fois que vous avez défini une pile TCP/IP pour l'adaptateur VMkernel, elle ne peut plus être modifiée. Si vous sélectionnez la pile TCP/IP de provisionnement ou vMotion, seule cette pile pourra être utilisée pour gérer le trafic de provisionnement ou vMotion sur l'hôte. Tous les adaptateurs VMkernel pour vMotion sur la pile TCP/IP par défaut sont désactivés pour les prochaines sessions vMotion. Si vous utilisez la pile TCP/IP de provisionnement, les adaptateurs VMkernel sur la pile TCP/IP par défaut sont désactivés, et vous ne pouvez pas effectuer certaines opérations. Ces opérations comprennent le trafic de provisionnement, comme la migration à froid de machines virtuelles, le clonage et la migration de snapshot.

- 7 (Facultatif) Sélectionnez les services à activer pour la pile TCP/IP par défaut sur l'hôte.

vMotion permet à l'adaptateur VMkernel de s'annoncer à un autre hôte comme la connexion réseau par laquelle le trafic vMotion est envoyé. Vous ne pouvez pas effectuer de migrations vers les hôtes sélectionnés à l'aide de vMotion si le service vMotion n'est activé pour aucun adaptateur VMkernel sur la pile TCP/IP par défaut ou si aucun adaptateur n'utilise la pile TCP/IP vMotion.

- 8 Passez vos sélections de paramètres en revue et cliquez sur **Créer**.

## Modifier les paramètres des adaptateurs réseau VMkernel dans VMware Host Client

Vous pouvez être amené à modifier le type de trafic pris en charge pour un adaptateur réseau VMkernel ou le mode d'obtention des adresses IPv4 ou IPv6.

### Procédure

- 1 Cliquez sur **Mise en réseau** dans l'inventaire VMware Host Client et cliquez sur **Cartes réseau VMkernel**.
- 2 Sélectionnez l'adaptateur VMkernel qui se trouve sur le commutateur cible standard, cliquez sur **Actions** et sélectionnez **Modifier les paramètres** dans le menu déroulant.
- 3 (Facultatif) Modifiez l'ID VLAN.

L'ID VLAN détermine le VLAN que le trafic réseau de l'adaptateur VMkernel utilisera.

- 4 (Facultatif) Pour modifier la version IP, sélectionnez IPv4, IPv6 ou les deux dans le menu déroulant.

**Note** L'option IPv6 n'apparaît pas sur les hôtes sur lesquels l'option IPv6 n'est pas activée.

- 5 (Facultatif) Développez la section des paramètres IPv4 pour sélectionner une option permettant d'obtenir des adresses IP.

| Option  | Description  |
|---|--|
| Utilisez DHCP pour obtenir les paramètres IP. | Les paramètres IP sont obtenus automatiquement. Un serveur DHCP doit être présent sur le réseau.   |
| Utiliser des paramètres IP statiques          | Entrez l'adresse IPv4 et un masque de sous-réseau pour l'adaptateur VMkernel.<br><br>Les adresses de la passerelle par défaut VMkernel et du serveur DNS pour IPv4 proviennent de la pile TCP/IP sélectionnée. |

- 6 (Facultatif) Développez la section des paramètres IPv6 pour sélectionner une option permettant d'obtenir des adresses IPv6.

| Option                    | Description  |
|---------------------------|--|
| DHCPv6                    | Utilisez DHCP pour obtenir les adresses IPv6. Un serveur DHCPv6 doit être présent sur le réseau.   |
| Configuration automatique | Utilisez une annonce de routage pour obtenir les adresses IPv6.  |
| Adresses IPv6 statiques   | a Cliquez sur <b>Ajouter une adresse</b> pour ajouter une adresse IPv6.<br>b Entrez l'adresse IPv6 et la longueur du préfixe de sous-réseau. |

- 7 (Facultatif) Sélectionnez le service à activer ou désactiver pour la pile TCP/IP par défaut sur l'hôte.

vMotion permet à l'adaptateur VMkernel de s'annoncer à un autre hôte comme la connexion réseau par laquelle le trafic vMotion est envoyé. Il est impossible d'effectuer des migrations vers les hôtes sélectionnés à l'aide de vMotion si le service vMotion n'est activé pour aucun adaptateur VMkernel sur la pile TCP/IP par défaut ou si aucun adaptateur n'utilise la pile TCP/IP vMotion.

- 8 Vérifiez les modifications de vos paramètres et cliquez sur **Enregistrer** pour appliquer vos modifications.

## Supprimer un adaptateur réseau VMkernel dans VMware Host Client

Dans VMware Host Client, vous pouvez supprimer un adaptateur réseau VMkernel si vous n'en avez plus besoin.

### Procédure

- 1 Cliquez sur **Mise en réseau** dans l'inventaire VMware Host Client et cliquez sur **Cartes réseau VMkernel**.

- 2 Cliquez avec le bouton droit sur l'adaptateur réseau VMkernel que vous voulez supprimer, puis cliquez sur **Supprimer**.
- 3 Cliquez sur **Supprimer** pour supprimer l'adaptateur réseau.

## Afficher la configuration des piles TCP/IP sur un hôte dans VMware Host Client

Vous pouvez également afficher le DNS et la configuration de routage de la pile TCP/IP d'un hôte, de même que les tables de routage IPv4 et IPv6, l'algorithme de contrôle d'encombrement et le nombre maximal de connexions autorisées.

### Procédure

- 1 Cliquez sur **Mise en réseau** dans l'inventaire hôte et cliquez sur **Piles TCP/IP**.
- 2 Cliquez sur une pile de la liste.

Les paramètres de configuration de la pile que vous avez sélectionnée apparaissent.

## Modifier la configuration d'une pile TCP/IP sur un hôte dans VMware Host Client

Vous pouvez modifier le DNS et la configuration de passerelle par défaut de la pile TCP/IP d'un hôte, de même que l'algorithme de contrôle d'encombrement, le nombre maximal de connexions autorisées et le nom des piles TCP/IP personnalisées.

### Procédure

- 1 Cliquez sur **Mise en réseau** dans l'inventaire VMware Host Client et cliquez sur **Piles TCP/IP**.
- 2 Cliquez avec le bouton droit sur une pile dans la liste et sélectionnez **Modifier les paramètres**.  
La boîte de dialogue Modifier la configuration TCP/IP - Pile de provisionnement s'ouvre.
- 3 Indiquez la manière dont l'hôte doit obtenir les paramètres pour cette pile TCP/IP.
  - Sélectionnez le bouton radio **Utiliser les services DHCP de l'adaptateur suivant** et sélectionnez l'adaptateur d'où proviendra la configuration des paramètres par défaut pour la pile TCP/IP.



- Sélectionnez **Configurer manuellement les paramètres pour cette pile TCP/IP** pour modifier la configuration des paramètres.

| Option                | Description   |
|-----------------------|---|
| Configuration de base | <b>Nom d'hôte</b><br>Modifiez le nom de votre hôte local.   |
|                       | <b>Nom de domaine</b><br>Modifiez le nom du domaine.  |
|                       | <b>Serveur DNS principal</b><br>Entrez une adresse IP du serveur DNS préférée.  |
|                       | <b>Serveur DNS secondaire</b><br>Entrez l'adresse IP d'un autre serveur DNS.  |
|                       | <b>Domaines de recherche</b><br>Spécifiez les suffixes DNS à utiliser dans la recherche de DNS lors de la résolution des noms de domaine incomplets.                  |
| Routage               | Modifiez les informations de passerelle IPv4 et IPv6.<br><br><b>Note</b> La suppression de la passerelle par défaut peut provoquer la perte de la connexion à l'hôte. |
| Paramètres avancés    | Modifiez l'algorithme de contrôle de l'encombrement et le nombre maximal de connexions.   |

4 Cliquez sur **Enregistrer**.

## Configurer le pare-feu ESXi dans VMware Host Client

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

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

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

## Gérer les paramètres du pare-feu ESXi à l'aide de VMware Host Client

Quand vous êtes connecté à un hôte ESXi avec VMware Host Client, vous pouvez configurer les connexions de pare-feu entrantes et sortantes pour un agent de service ou de gestion.

---

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

---

### Procédure

- 1 Cliquez sur **Mise en réseau** dans l'inventaire VMware Host Client.
- 2 Cliquez sur **Règles du pare-feu**.  
  
VMware Host Client affiche la liste des connexions entrantes et sortantes actives avec les ports de pare-feu correspondants.
- 3 Pour certains services, vous pouvez gérer les détails du service. Cliquez avec le bouton droit sur un service et sélectionnez une option dans le menu contextuel.
  - Utilisez les boutons Démarrer, Arrêter ou Redémarrer pour modifier temporairement l'état d'un service.
  - Modifiez la stratégie de démarrage pour configurer le service afin qu'il démarre et s'arrête avec l'hôte, les ports de pare-feu ou manuellement.

## Ajouter des adresses IP autorisées pour ESXi Host avec VMware Host Client

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

### Procédure

- 1 Cliquez sur **Mise en réseau** dans l'inventaire VMware Host Client et cliquez sur **Règles des pare-feu**.
- 2 Cliquez sur un service dans la liste, puis cliquez sur **Modifier les paramètres**.
- 3 Dans la section Adresses IP autorisées, cliquez sur **Autoriser uniquement les connexions des réseaux suivants**, puis saisissez les adresses IP des réseaux que vous souhaitez connecter à l'hôte.

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

- 192.168.0.0/24
- 192.168.1.2, 2001::1/64

- fd3e:29a6:0a81:e478::/64

4 Cliquez sur **OK**.

## Surveiller des événements et tâches de mise en réseau dans VMware Host Client

Vous pouvez afficher les informations sur les événements et tâches associés aux groupes de ports, commutateurs virtuels, adaptateurs réseau physiques, adaptateurs réseau VMkernel et piles TCP/IP sur l'hôte ESXi que vous gérez.

### Surveiller les groupes de ports dans VMware Host Client

Dans VMware Host Client, vous pouvez surveiller les performances des groupes de ports en affichant les événements et tâches des groupes de ports sur l'hôte.

#### Procédure

- 1 Cliquez sur **Mise en réseau** dans l'inventaire VMware Host Client.
- 2 Cliquez sur **Groupes de ports**.
- 3 Cliquez sur un groupe de ports de la liste.  
Le groupe de ports se développe dans l'inventaire VMware Host Client.
- 4 Cliquez sur **Surveiller** sous le nom du groupe de ports dans l'inventaire VMware Host Client.
- 5 (Facultatif) Cliquez sur **Événements** pour afficher les événements associés au groupe de ports.

### Surveiller les commutateurs virtuels dans VMware Host Client

Dans VMware Host Client, vous pouvez surveiller les performances des commutateurs virtuels en affichant les événements et tâches des commutateurs virtuels sur l'hôte.

#### Procédure

- 1 Cliquez sur **Mise en réseau** dans l'inventaire VMware Host Client.
- 2 Cliquez sur **Commutateurs virtuel**.
- 3 Sélectionnez un commutateur virtuel dans la liste.  
Le commutateur virtuel apparaît dans l'inventaire VMware Host Client.
- 4 Cliquez sur **Surveiller** sous le nom du commutateur virtuel dans l'inventaire VMware Host Client.
- 5 (Facultatif) Cliquez sur **Événements** pour afficher les événements associés au commutateur virtuel.

## Surveiller des adaptateurs réseau physiques dans VMware Host Client

Dans VMware Host Client, vous pouvez surveiller les performances des cartes réseau physiques (NIC) en affichant les événements et tâches des cartes réseau physiques sur l'hôte.

### Procédure

- 1 Cliquez sur **Mise en réseau** dans l'inventaire VMware Host Client.
- 2 Cliquez sur **Cartes réseau physiques**.
- 3 Cliquez sur un adaptateur réseau physique dans la liste.  
L'adaptateur réseau physique se développe dans l'inventaire VMware Host Client.
- 4 Cliquez sur **Surveiller** sous le nom de l'adaptateur réseau physique dans l'inventaire VMware Host Client.
- 5 (Facultatif) Cliquez sur **Événements** pour afficher les événements associés à l'adaptateur réseau physique.

## Surveiller des adaptateurs réseau VMkernel dans VMware Host Client

Dans VMware Host Client, vous pouvez surveiller les performances des adaptateurs réseau VMkernel en affichant les événements et tâches des adaptateurs réseau VMkernel sur l'hôte.

### Procédure

- 1 Cliquez sur **Mise en réseau** dans l'inventaire VMware Host Client.
- 2 Cliquez sur **Adaptateurs réseau VMkernel**.
- 3 Cliquez sur un adaptateur réseau VMkernel dans la liste.  
L'adaptateur réseau VMkernel se développe dans l'inventaire VMware Host Client.
- 4 Cliquez sur **Surveiller** sous le nom de l'adaptateur réseau VMkernel dans l'inventaire VMware Host Client.
- 5 (Facultatif) Cliquez sur **Événements** pour afficher les événements associés à l'adaptateur réseau VMkernel.

## Surveiller les piles TCP/IP dans VMware Host Client

Dans VMware Host Client, vous pouvez surveiller les performances des piles TCP/IP en affichant les événements et tâches des piles TCP/IP sur l'hôte.

### Procédure

- 1 Cliquez sur **Mise en réseau** dans l'inventaire VMware Host Client.
- 2 Cliquez sur **Piles TCP/IP**.

- 3 Cliquez sur une pile TCP/IP dans la liste.

La pile TCP/IP se développe dans l'inventaire VMware Host Client.

- 4 Cliquez sur **Surveiller** sous le nom de la pile TCP/IP dans l'inventaire VMware Host Client.
- 5 (Facultatif) Cliquez sur **Événements** pour afficher les événements associés à la pile TCP/IP.
- 6 (Facultatif) Cliquez sur **Tâches** pour afficher les tâches associées à la pile TCP/IP.