Guide d'administration de VMware Horizon FLEX

Horizon FLEX 1.6

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

FR-001873-00

vmware®

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

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

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

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

docfeedback@vmware.com

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

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

Table des matières

Guide d'administration de VMware Horizon FLEX

Le *Guide d'administration de VMware Horizon FLEX* décrit comment installer et gérer VMware Horizon® FLEX™.

Public visé

Ces informations sont destinées à toutes les personnes qui souhaitent installer Horizon FLEX. Les informations sont rédigées pour les administrateurs de système d'exploitation Windows expérimentés qui connaissent bien la technologie des machines virtuelles.

Présentation d' Horizon FLEX 1

Horizon FLEX est une solution de poste de travail en conteneur basée sur des stratégies qui permet aux administrateurs informatiques de créer, de sécuriser et de gérer des postes de travail locaux pour des utilisateurs finaux. Les utilisateurs finaux travaillent sur une machine virtuelle limitée, appelée machine virtuelle Horizon FLEX, sur leurs propres ordinateurs. Comme les machines virtuelles Horizon FLEX sont stockées localement, sur des ordinateurs d'utilisateurs finaux, les applications d'entreprise sont accessibles pour les utilisateurs hors ligne.

Ce chapitre aborde les rubriques suivantes :

Composants d' Horizon FLEX

Horizon FLEX est une combinaison de composants VMware, incluant Mirage, Fusion Pro et Workstation Player.

VMware Mirage® pour Horizon FLEX
Le Mirage Server utilisé par Horizon FLEX. Le serveur offre la gestion de machine virtuelle Horizon FLEX. Vous pouvez gérer, sauvegarder et corriger des machines virtuelles en utilisant la technologie de superposition Mirage pour Horizon FLEX. L'utilisation de Mirage pour Horizon FLEX est facultative. Vous pouvez également utiliser d'autres outils de gestion d'images pour gérer des machines virtuelles Horizon FLEX.

Serveur de stratégie Horizon FLEX
Le Mirage Server standard avec une extension qui inclut une fonctionnalité spécifique d'Horizon FLEX. Le Serveur de stratégie Horizon FLEX est activé lorsque vous appliquez la licence Horizon FLEX sur Mirage pour Horizon FLEX.

Console d'administration Horizon FLEX
L'interface utilisateur de gestion Web du Serveur de stratégie Horizon FLEX. La Console d'administration Horizon FLEX se trouve dans le composant Mirage Web Manager. Vous utilisez la Console d'administration Horizon FLEX pour exécuter des tâches de gestion de machine virtuelle, notamment :

- Gérer un inventaire de machines virtuelles

- Parcourir une liste d'utilisateurs et de groupes dans le service Active Directory
- Accorder des droits à des utilisateurs et des groupes sur une ou plusieurs machines virtuelles
- Spécifier des stratégies de machine virtuelle pour un droit donné
- Empêcher les utilisateurs d'accéder à des machines virtuelles en utilisant un verrou à distance
- Examiner les détails et l'état des machines virtuelles à tout moment

Horizon FLEX Client

Le logiciel client que les utilisateurs finaux utilisent pour télécharger les machines virtuelles Horizon FLEX sur leurs ordinateurs locaux. Les clients incluent VMware Fusion Pro® pour ordinateurs Mac et VMware Workstation Player™ pour ordinateurs Windows. Fusion Pro et Workstation Player ne sont pas inclus dans le package Horizon FLEX. Une clé de licence est fournie pour Fusion Pro et Workstation Player.

Machine virtuelle Horizon FLEX

La machine virtuelle que les utilisateurs finaux exécutent sur leurs propres ordinateurs. Vous utilisez Fusion Pro pour créer des machines virtuelles sources pour des machines virtuelles Horizon FLEX. Fusion Pro est inclus dans le package Horizon FLEX. Un Horizon FLEX Server peut prendre en charge jusqu'à 1 000 utilisateurs.

Remarque Vous pouvez également utiliser VMware Workstation Pro™ pour créer des machines virtuelles sources. Workstation Pro n'est pas inclus dans le package Horizon FLEX.

À propos de Mirage

Mirage fait partie intégrante du fonctionnement et de l'utilisation des machines virtuelles Horizon FLEX.

Horizon FLEX utilise un sous-ensemble des fonctionnalités disponibles dans Mirage :

- Serveur Mirage
  - Mirage Management Server
- Mirage Web Manager
  - Console de gestion Mirage

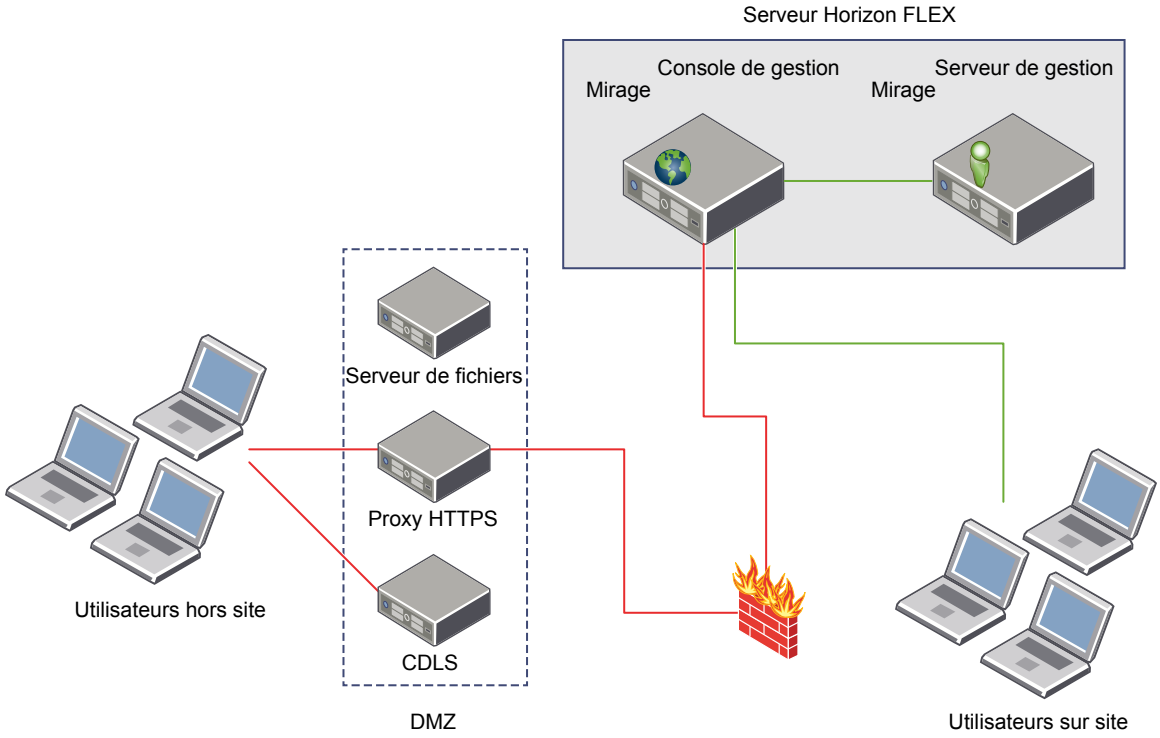
Ce document ne décrit pas toutes les informations concernant Mirage. Pour obtenir des informations complètes sur Mirage, consultez la documentation de Mirage à l'adresse https://www.vmware.com/support/pubs/mirage_pubs.html.

Architecture d' Horizon FLEX

Un déploiement typique d'Horizon FLEX inclut le Horizon FLEX Server, un serveur de fichiers, un proxy HTTPS, un contrôleur de domaine en lecture seule (CDLS) et des systèmes d'utilisateurs finaux hors site et sur site.

Figure 1-1 montre la relation entre les principaux composants d'un déploiement d'Horizon FLEX.

Figure 1-1. Exemple de déploiement d' Horizon FLEX sans Mirage



Serveur Horizon FLEX

Le Horizon FLEX Server se compose de la console d'administration Horizon FLEX et du serveur de stratégie Horizon FLEX. Le Horizon FLEX Server offre la fonctionnalité suivante.

- Il affecte des machines virtuelles Horizon FLEX à des utilisateurs et des groupes à partir d'un service d'annuaire
- Il conserve un enregistrement des machines virtuelles Horizon FLEX utilisées par des utilisateurs individuels
- Il offre la gestion des certificats de sécurité pour assurer une communication sécurisée et approuvée entre les machines virtuelles Horizon FLEX déployées et le Horizon FLEX Server.
- Il applique des paramètres de stratégie sur le client
- Il autorise la modification de paramètres de stratégie pour une combinaison utilisateur et machine virtuelle Horizon FLEX donnée
- Il surveille l'état de la machine virtuelle Horizon FLEX

La console de gestion Mirage est l'interface utilisateur graphique utilisée pour la maintenance, la gestion et la surveillance évolutives des points de terminaison déployés. Le gestionnaire Web Mirage reproduit la fonctionnalité de la console de gestion Mirage.

Par défaut, le port 7443 est utilisé par le serveur de stratégie Horizon FLEX pour l'accès externe et le port 8443 est utilisé par le serveur de gestion Mirage pour communiquer avec le serveur de stratégie Horizon FLEX. Vous devez configurer vos stratégies de pare-feu pour autoriser les ports requis. Pour voir une liste complète des ports utilisés par Mirage, consultez la documentation de Mirage à l'adresse https://www.vmware.com/support/pubs/mirage_pubs.html.

Serveur de fichiers

Un serveur de fichiers stocke les fichiers TAR qui contiennent les fichiers de la machine virtuelle source pour les machines virtuelles Horizon FLEX. Le serveur de fichiers peut se trouver sur tout serveur auquel un utilisateur client peut accéder sans entrer d'informations d'identification. Le serveur de fichiers est situé dans la zone DMZ dans cet exemple, mais il ne s'agit pas d'une obligation.

Proxy HTTPS

Un proxy HTTPS permet à des systèmes d'utilisateurs finaux hors site d'atteindre la console de gestion Mirage et d'obtenir des mises à jour de stratégie.

CDLS

Un CDLS permet à des systèmes d'utilisateurs finaux hors site d'ouvrir une session sur leurs machines virtuelles Horizon FLEX et de joindre le domaine Active Directory pour le premier démarrage de la VM. Un CDLS est requis uniquement si vous autorisez les utilisateurs extérieurs à se connecter sans utiliser de VPN. Le CDLS se trouve dans la DMZ.

Équilibrage de charge

Horizon FLEX prend en charge l'équilibrage de charge à l'aide de plusieurs serveurs de stratégie. Configurez un serveur Windows actif/passif défini pour la tolérance aux pannes pour votre topologie Horizon FLEX.

Configuration requise d' Horizon FLEX

Chaque produit dans le package Horizon FLEX a une certaine configuration requise.

Configuration requise pour le serveur Horizon FLEX et le serveur Mirage	Pour plus d'informations, consultez « Configuration système requise pour Horizon FLEX Server », page 11.
Mirage pour Horizon FLEX	La configuration système requise d'Horizon FLEX 1.6 est la même que pour Mirage 5.5. Consultez la documentation de Mirage à l'adresse https://www.vmware.com/support/pubs/mirage_pubs.html.
Horizon FLEX Client pour Mac	Horizon FLEX 1.6 utilise Fusion Pro 8.0 comme logiciel client pour les clients Mac. Horizon FLEX 1.6 n'est pas compatible avec les versions antérieures de Fusion Pro. Pour les exigences matérielles et logicielles de Fusion Pro, consultez le *Guide de l'utilisateur de VMware Horizon FLEX Client*.
Horizon FLEX Client pour Windows	Horizon FLEX 1.6 utilise Workstation Player 12.0 comme logiciel client pour les clients Windows. Horizon FLEX 1.6 n'est pas compatible avec les versions antérieures de Player Pro. Pour les exigences matérielles et logicielles de Workstation Player, consultez le *Guide de l'utilisateur de VMware Horizon FLEX Client*.
Workstation Pro	Vous pouvez utiliser Workstation Pro 12.0 pour créer et ouvrir une machine virtuelle source, mais Workstation Pro ne peut pas télécharger une machine virtuelle Horizon FLEX. Workstation Pro n'est pas inclus dans le module d'installation d' Horizon FLEX.

Pour les exigences matérielles et logicielles de Workstation Pro, consultez la documentation de Workstation Pro à l'adresse https://www.vmware.com/support/pubs/ws_pubs.html.

Configuration système requise pour Horizon FLEX Server

L'environnement Horizon FLEX inclut une configuration système requise pour le serveur Horizon FLEX Server et pour le serveur Mirage.

Configuration système requise pour Horizon FLEX Server

- CPU minimal : 1 processeur à quatre cœurs ou 2 vCPU
- Vitesse du cœur Intel de 2,26 GHz ou équivalent
- RAM minimale : 512 Mo avec 4 Go recommandés
- Espace disque minimal : 10 Go+, 40 Go+ recommandés
- Windows 2008 R2, Windows 2012 ou version ultérieure
- .NET 4.5.1 et versions ultérieures
- IIS 7.0+ avec compatibilité avec la gestion IIS 6, avec ASP et ASP.NET
- Active Directory : compte d'administrateur avec autorisations d'ajouter des objets d'ordinateur au domaine
- SQL 2008 Express ou SQL Server 2008 (requis pour l'installation de Mirage)
- Partage de fichiers HTTP ou répertoire virtuel IIS avec de l'espace disponible pour les machines virtuelles sources
- Ports de pare-feu pour la console d'administration d'Horizon FLEX
  - Ports par défaut d'IIS et de l'application Web Horizon FLEX : HTTP - 7080, HTTPS - 7443 (Les appels dirigés vers le port HTTP sont redirigés vers le port HTTPS.)
  - Le serveur de gestion Mirage écoute les demandes de Windows Communication Foundation (WCF) sur le port suivant : HTTP - 8443
- Un certificat est requis pour le serveur Horizon FLEX Server si SSL est utilisé.

Configuration requise pour le serveur Mirage

- CPU minimal : 4 vCPU avec 8 vCPU recommandés
- RAM minimale : 8 Go avec 16 Go recommandés
- 146 Go d'espace disque libre
- Windows 2008 R2, Windows 2012 ou version ultérieure
- .NET 4.5.1 et versions ultérieures

Configuration réseau requise d' Horizon FLEX

Horizon FLEX permet aux utilisateurs finaux d'exécuter des applications d'entreprise même lorsqu'ils sont déconnectés du réseau. Des machines virtuelles Horizon FLEX sont stockées localement, il n'est donc pas nécessaire d'avoir une connexion réseau pour utiliser complètement le poste de travail.

Une connexion réseau est requise entre le Serveur de stratégie Horizon FLEX et le Horizon FLEX Client dans les circonstances suivantes :

- Pour le premier téléchargement de la machine virtuelle Horizon FLEX sur l'ordinateur local de l'utilisateur.
- Pour enregistrer une machine virtuelle Horizon FLEX qui était fournie sur un périphérique USB ou déployée sur l'ordinateur local de l'utilisateur.
- Pour recevoir des restrictions de machine virtuelle ou des mises à jour de stratégie d'Horizon FLEX.

Lorsque vous enregistrez une machine virtuelle source pour une machine virtuelle Horizon FLEX, vous spécifiez l'URL de l'emplacement de téléchargement pour un package de machine virtuelle. Le dossier de téléchargement doit être accessible sur les ordinateurs des utilisateurs finaux pour télécharger des machines virtuelles.

Systèmes d'exploitation hôtes et invités pris en charge

L'ordinateur local sur lequel les utilisateurs finaux utilisent le Horizon FLEX Client doit contenir un système d'exploitation hôte pris en charge. Une machine virtuelle Horizon FLEX doit utiliser un système d'exploitation invité pris en charge.

Systèmes d'exploitation hôtes pris en charge

Vos utilisateurs finaux peuvent exécuter le Horizon FLEX Client et accéder à leur machine virtuelle Horizon FLEX en utilisant un ordinateur physique avec l'un des systèmes d'exploitation suivants.

Tableau 1-1. Systèmes d'exploitation hôtes pris en charge

Horizon FLEX Client	Systèmes d'exploitation pris en charge
Workstation Player	■ Windows 7 ■ Windows 8.1 Enterprise ■ Windows Server 2012 R2 ■ Windows 8 ■ Windows 8.1 Pro ■ Windows 10 **Remarque** Workstation Player ne prend charge que les systèmes d'exploitation 64 bits.
Fusion Pro	■ Mac OS X 10.11 ■ Mac OS X 10.10 ■ Mac OS X 10.9

Systèmes d'exploitation invités pris en charge

Une machine virtuelle Horizon FLEX peut contenir l'un des systèmes d'exploitation invités suivants.

- Windows 10
- Windows 8.1
- Windows 7
- Windows XP

- Windows Server 2012 R2
- Ubuntu 14.04

Installation d' Horizon FLEX 2

L'installation d'Horizon FLEX implique d'installer les composants de serveur et de client Horizon FLEX, de créer des dossiers pour stocker des machines virtuelles Horizon FLEX, de préparer Active Directory, de configurer des certificats et de créer et déployer des machines virtuelles Horizon FLEX.

Ce chapitre aborde les rubriques suivantes :

Aperçu de l'installation d' Horizon FLEX

Horizon FLEX est une combinaison de composants VMware, incluant Mirage, Fusion Pro et Workstation Player. L'installation d'Horizon FLEX implique l'installation de chacun de ces composants et l'exécution de tâches spécifiques d'Horizon FLEX supplémentaires. Pour un déploiement réussi d' Horizon FLEX, vous devez comprendre l'ordre des tâches requises.

Avant d'installer Horizon FLEX, vérifiez qu'il répond à toutes les exigences matérielles et logicielles, que vous disposez des licences valides et que vous avez téléchargé les programmes d'installation des composants d'Horizon FLEX sur la page de téléchargement de produit de VMware Horizon FLEX.

Vous installez Horizon FLEX en exécutant ces étapes :

1 Installez le système Mirage.

  Reportez-vous à « Installation et configuration de composants Mirage pour Horizon FLEX », page 16.

2 Configurez les certificats des machines virtuelles Horizon FLEX.

  Reportez-vous à Chapitre 3, « Configuration de certificats pour des machines virtuelles Horizon FLEX », page 25.

3 Créez un dossier de téléchargement pour stocker vos packages de machine virtuelle Horizon FLEX.

  Reportez-vous à « Créer un dossier de téléchargement pour des packages de machine virtuelle Horizon FLEX », page 17.

4 Ajoutez un répertoire virtuel dans IIS pour le dossier de téléchargement de machine virtuelle Horizon FLEX et modifiez les liaisons de site.

   Reportez-vous à « Configurer le certificat de serveur SSL IIS pour le Horizon FLEX Server », page 18.

5 (Facultatif) Configurez Horizon FLEX pour synchroniser des entités uniquement dans une unité d'organisation (UO) Active Directory sélectionnée.

   Reportez-vous à « Configurer les paramètres Active Directory », page 19.

6 Testez la connexion à la Console d'administration Horizon FLEX.

   Reportez-vous à « Tester la connexion Console d'administration Horizon FLEX », page 20.

7 Installez un Horizon FLEX Client sur chaque hôte d'utilisateur final ou demandez aux utilisateurs finaux d'installer un Horizon FLEX Client sur leurs propres ordinateurs.

   Reportez-vous à « Installation d'Horizon FLEX Client pour des utilisateurs finaux », page 20.

8 Créez et déployez des machines virtuelles Horizon FLEX.

   Reportez-vous à Chapitre 4, « Création et déploiement de machines virtuelles Horizon FLEX », page 35.

Installation et configuration de composants Mirage pour Horizon FLEX

La première étape d'installation d'Horizon FLEX consiste à installer et à configurer le système Mirage.

Le package Horizon FLEX inclut les composants suivants :

- VMware Mirage pour Horizon FLEX (logiciel principal de Mirage)
- Mirage PowerCLI pour Windows
- Mirage Gateway Appliance Software

Téléchargez les fichiers d'installation sur la page de téléchargement de produit de Horizon FLEX Server.

Le déploiement de Mirage implique l'installation des composants suivants.

1 Serveur de gestion d'Mirage

2 Serveur Mirage

3 Mirage Management Console

4 Mirage Web Manager

Pour installer et configurer le système Mirage, suivez les instructions d'installation dans la documentation Mirage à l'adresse https://www.vmware.com/support/pubs/mirage_pubs.html.

Lorsque vous installez le système Mirage, vous devez sélectionner certaines options pour que le Horizon FLEX Server fonctionne correctement.

- Le serveur Mirage et la console Mirage ne sont requis que si vous installez le client Mirage sur les machines virtuelles source.
- Si vous placez les images de machine virtuelle sur le même système que Horizon FLEX Server, placez les images sur le serveur Web par défaut IIS.
- Le serveur de gestion Web et le serveur de gestion Mirage peuvent être installés sur le même serveur, mais leur installation sur des serveurs différents améliore l'évolutivité. Le serveur SQL Server doit être installé sur un serveur séparé du serveur de gestion Web et du serveur de gestion Mirage.

- Lors de l'installation du serveur Mirage, choisissez SSL pour le transport du serveur Mirage. SSL est requis pour utiliser la fonction de passerelle Mirage pour l'accès externe et la gestion des systèmes Horizon FLEX. Avant de configurer le serveur Mirage pour SSL, vous devez installer le certificat SSL du serveur.
- Avant d'installer Mirage Web Manager, vérifiez que .NET Framework 4.5.1 est installé sur le serveur.
- Mirage Management Server doit être exécuté en tant qu'utilisateur avec des autorisations de lecture Active Directory. Si vous prévoyez de joindre des machines virtuelles Horizon FLEX à un domaine Active Directory, Mirage Management Server doit être exécuté en tant qu'utilisateur avec des autorisations de jonction de domaine.

Créer un dossier de téléchargement pour des packages de machine virtuelle Horizon FLEX

Lors du processus de déploiement de machine virtuelle d'Horizon FLEX, vous comprimez vos packages de machine virtuelle source au format TAR (`.tar`) pour que les utilisateurs puissent facilement télécharger leurs machines virtuelles Horizon FLEX. Vous devez créer un dossier de téléchargement pour stocker ces fichiers TAR.

Procédure

1 Créez le dossier de téléchargement sur le Horizon FLEX Server ou sur un autre serveur.

   Il n'est pas nécessaire que le dossier de téléchargement se trouve sur Horizon FLEX Server, mais les fichiers qu'il contient doivent être téléchargeables sans demande d'authentification. Si vous créez le dossier de téléchargement sur le même serveur IIS que le serveur Horizon FLEX, vous pouvez créer le dossier sous le même dossier racine de document IIS par défaut du site Web par défaut. Ne créez pas le dossier de téléchargement sous le site Web de gestion de VMware Mirage.

2 Affectez des autorisations au dossier de téléchargement pour que les utilisateurs puissent télécharger les fichiers qu'il contient.

3 (Facultatif) Partagez le dossier de téléchargement avec un groupe d'administration, tel que les administrateurs d'Horizon FLEX. Il peut s'agir d'un groupe d'administration pour que les utilisateurs gèrent les déploiements d'Horizon FLEX.

   Cette étape peut faciliter l'enregistrement de vos machines virtuelles sources avec le Serveur de stratégie Horizon FLEX.

Suivant

Reportez-vous à « Configurer le certificat de serveur SSL IIS pour le Horizon FLEX Server », page 18.

Configurer un certificat pour Horizon FLEX Server à l'aide d'OpenSSL

Vous pouvez créer un certificat auto-signé pour Horizon FLEX Server à l'aide d'OpenSSL.

Prérequis

Le fichier de configuration OpenSSL est créé sur le serveur Mirage Gateway. Consultez la documentation de Mirage à l'adresse https://www.vmware.com/support/pubs/mirage_pubs.html.

Procédure

1 À l'invite de commande OpenSSL, créez un certificat : **`$ openssl req –new –days expiration time –x509 –newkey rsa:2048 – keyout key filename –outcertificate filename –nodes`**

expiration time représente le nombre de jours pendant lesquels le certificat doit être valide, *key filename* représente le nom de fichier de la clé et *certificate filename* représente le nom du nouveau certificat.

Un certificat auto-signé et une clé privée sont générés. Le certificat utilise une clé RSA 2 048 bits et ne protège pas la clé avec une phrase de passe.

2 Lorsque vous y êtes invité, entrez le nom du pays, le nom de l'état, la localité, le nom de l'entreprise et le nom de l'unité d'organisation.

3 Dans la zone de texte Nom commun, entrez le nom d'hôte d'Horizon FLEX Server à protéger.

Cette zone de texte doit être remplie.

4 Entrez l'adresse e-mail.

Le certificat auto-signé et la clé privée associée sont générés.

5 Si la clé privée doit être au format `.pfx`, entrez la commande suivante à l'aide du nom de certificat et du nom de fichier de clé générés dans les étapes précédentes :
`$ openSSL pkcs12 –export –outoutput pfx filename –inkey key filename –in certificate name`

Un nouveau fichier `.pfx` protégé par mot de passe est généré et peut être déployé sur tout périphérique nécessitant des certificats `.pfx` plutôt que des certificats PEM.

Configurer le certificat de serveur SSL IIS pour le Horizon FLEX Server

Vous devez configurer le certificat de serveur SSL IIS pour Horizon FLEX Server afin de définir la chaîne de certificats entre Horizon FLEX Server et les machines virtuelles Horizon FLEX.

Prérequis

- Installez Mirage pour Horizon FLEX. Reportez-vous à « Installation et configuration de composants Mirage pour Horizon FLEX », page 16.
- Installez le certificat de serveur SSL sur le Mirage Server. Consultez la documentation de Mirage à l'adresse https://www.vmware.com/support/pubs/mirage_pubs.html
- Configurez l'authentification de certificat pour vos machines virtuelles Horizon FLEX. Reportez-vous à Chapitre 3, « Configuration de certificats pour des machines virtuelles Horizon FLEX », page 25.
- Créez un dossier de téléchargement pour vos packages de machine virtuelle Horizon FLEX. Reportez-vous à « Créer un dossier de téléchargement pour des packages de machine virtuelle Horizon FLEX », page 17.

Procédure

1 Ouvrez IIS Manager.

2 Accédez au **Site Web de gestion de VMware Mirage** et sélectionnez l'emplacement du dossier de téléchargement.

3 Cliquez avec le bouton droit sur l'emplacement du dossier et sélectionnez **Ajouter un répertoire virtuel**.

4 Saisissez un nom dans la zone de texte **Alias**, accédez au dossier que vous avez créé pour contenir les packages de machine virtuelle Horizon FLEXet cliquez sur **OK**.

5 Accédez au nœud racine, le nœud de connexion défini pour le Mirage Server.

6 Sur la page Accueil de Mirage, sous IIS, double-cliquez sur **Certificats de serveur**.

La fenêtre Certificats de serveur SSL IIS s'ouvre.

7 Cliquez sur **Importer** dans la colonne de droite.

Cette étape importe le certificat SSL créé et affecte une clé pour identifier le certificat.

8 Sélectionnez **Site Web de gestion de VMware Mirage** et cliquez sur **Modifier les liaisons** dans la colonne de droite.

9 Définissez le port HTTPS pour utiliser votre certificat de Horizon FLEX Server et cliquez sur **OK**.

Configurer les paramètres Active Directory

Lorsque vous accordez des droits à une machine virtuelle Horizon FLEX, vous ajoutez des utilisateurs et des groupes de votre infrastructure Active Directory existante au droit. Par défaut, Horizon FLEX synchronise toute votre infrastructure Active Directory avec la base de données Horizon FLEX. Vous pouvez éventuellement configurer Horizon FLEX pour ne synchroniser qu'une unité d'organisation (UO) spécifique.

Prérequis

Installez Mirage pour Horizon FLEX. Reportez-vous à « Installation et configuration de composants Mirage pour Horizon FLEX », page 16.

Procédure

1 Démarrez la Console d'administration Horizon FLEX.

a Dans un navigateur Web, entrez **`https://`*`WebManagerServer`*`:7443/rvm`**, où *WebManagerServer* est le nom DNS ou l'adresse IP de l'hôte où Mirage Web Manager est installé.

b Entrez le nom d'utilisateur et le mot de passe d'un compte de domaine ayant accès à Mirage.

c Cliquez sur **Connexion**.

2 Dans la Console d'administration Horizon FLEX, cliquez sur l'icône **Paramètres système généraux** et cliquez sur **Paramètres Active Directory**.

3 Saisissez l'UO à synchroniser dans la zone de texte **Unité d'organisation**.

Lorsque vous commencez à saisir dans la zone de texte, les UO disponibles dans votre infrastructure Active Directory apparaissent dans un menu déroulant et vous pouvez sélectionner l'UO appropriée.

4 Cliquez sur **OK** pour enregistrer le paramètre de l'UO.

Le Horizon FLEX Server valide l'UO pour vérifier qu'elle existe et qu'elle est accessible.

Le Horizon FLEX Server synchronise les entités Active Directory qui appartiennent uniquement à l'UO que vous avez sélectionnée, y compris les entités qui appartiennent aux UO enfants de l'UO sélectionnée.

À chaque fois que vous configurez une nouvelle UO, le Horizon FLEX Server supprime les entités précédemment synchronisées à partir de la base de données et démarre un nouveau processus complet de synchronisation.

Vous pouvez configurer la stratégie des machines virtuelles clientes pour que le mot de passe de mise sous tension corresponde au mot de passe Active Directory de l'utilisateur après le premier démarrage. Reportez-vous à « Configurer une stratégie générale pour une image Horizon FLEX », page 44.

Tester la connexion Console d'administration Horizon FLEX

Vous pouvez vérifier votre déploiement d'Horizon FLEX en testant la connexion Console d'administration Horizon FLEX.

Prérequis

- Installez Mirage pour Horizon FLEX. Reportez-vous à « Installation et configuration de composants Mirage pour Horizon FLEX », page 16.
- Configurez l'authentification par certificat. Reportez-vous à Chapitre 3, « Configuration de certificats pour des machines virtuelles Horizon FLEX », page 25.

Procédure

1. Démarrez la Console d'administration Horizon FLEX.
   a. Dans un navigateur Web, entrez **`https://WebManagerServer:7443/rvm`**, où *WebManagerServer* est le nom DNS ou l'adresse IP de l'hôte où Mirage Web Manager est installé.
   b. Entrez le nom d'utilisateur et le mot de passe d'un compte de domaine ayant accès à Mirage.
   c. Cliquez sur **Connexion**.
2. Vérifiez que la page Console d'administration Horizon FLEX apparaît correctement.

   Les boutons **Images**, **Stratégies**, **Droits** et **Machines virtuelles** doivent être visibles dans le volet de navigation de gauche.

Installation d' Horizon FLEX Client pour des utilisateurs finaux

Le logiciel Horizon FLEX Client doit être installé sur les ordinateurs locaux des utilisateurs pour que ces derniers puissent télécharger les machines virtuelles Horizon FLEX. Les clients pris en charge inclus dans le package Horizon FLEX sont les machines Fusion Pro pour Mac OS X et les machines Workstation Player pour Windows.

Vous pouvez créer un déploiement en masse pour installer Horizon FLEX Client sur de nombreux systèmes à la fois ou vous pouvez demander aux utilisateurs d'obtenir Horizon FLEX Client sur le site Web de VMware et de l'installer eux-mêmes. Vous pouvez également exécuter une installation sans assistance de Workstation Player sur plusieurs machines Windows.

Créer un package de déploiement en masse pour installer Fusion Pro

Vous pouvez créer un package de déploiement en masse de Fusion Pro pour installer Fusion Pro sur plusieurs Macs d'utilisateurs finaux. Vous pouvez utiliser des outils de déploiement de package standard, notamment Apple Remote Desktop Admin, pour déployer le package de déploiement en masse.

Lorsque vous configurez le package de déploiement en masse, spécifiez votre clé de licence Horizon FLEX dans la section `[Volume License]` du fichier `Deploy.ini` et placez une copie de l'application Fusion Pro dans le dossier `00Fusion_Deployment_Items`.

Vous pouvez utiliser le paramètre facultatif `connectAtStartupURL` dans la section `[Locations]` du fichier `Deploy.ini` pour spécifier un nom d'utilisateur et le nom d'hôte de votre Horizon FLEX Server, par exemple :

```
connectAtStartupURL = vmware-rvm://johndoe@yourflexserver.com:7443
```

Si aucune machine virtuelle n'est installée sur le Mac de l'utilisateur lorsque l'utilisateur lance Fusion Pro, la boîte de dialogue Se connecter s'ouvre et les zones de texte **Serveur** et **Nom d'utilisateur** sont pré-remplies avec le nom d'hôte et le nom d'utilisateur que vous avez spécifiés dans le paramètre `connectAtStartupURL`.

Pour des informations détaillées sur la création d'un package de déploiement en masse, consultez l'article de la base de connaissances VMware à l'adresse http://kb.vmware.com/kb/2058680.

Fournir un module d'installation de Workstation Player à des utilisateurs finaux

Vous pouvez installer Workstation Player sur les machines d'utilisateur final à l'aide d'une ligne de commande et spécifier les paramètres de connexion du serveur Horizon FLEX Server à l'aide d'un URI (Uniform Resource Identifier). Lorsque l'installation de Workstation Player est terminée, l'utilisateur final est invité à se connecter à un serveur et à télécharger une machine virtuelle Horizon FLEX.

Prérequis

- Donnez à l'utilisateur final un mot de passe pour le serveur et la clé de licence de Workstation Player à utiliser avec Horizon FLEX.

Procédure

- Construisez un URI pour créer un module d'installation et de déploiement de Workstation Player personnalisé.

  La structure de la ligne de commande est la suivante :

  ```
  VMware-player-x.x.x-xxxxxxx.exe /v PLAYER_RVM_URI="vmware-rvm://username@myserver.com:7443"
  ```

  Spécifiez la version et le numéro de build du fichier .exe de Workstation Player. *username* est le nom de connexion de l'utilisateur et *myserver.com* est le nom d'hôte du serveur. Vous devez inclure `vmware-rvm://` et `:7443` dans l'adresse du serveur. N'incluez pas http ou https dans l'adresse du serveur.

Exécuter une installation sans assistance de Workstation Player

Vous pouvez utiliser la fonction d'installation sans assistance de Microsoft Windows Installer (MSI) pour installer Workstation Player sur plusieurs hôtes Windows sans avoir à répondre aux invites d'un assistant. Cette fonction est pratique dans une grande entreprise.

Prérequis

- Vérifiez que le système hôte répond à la configuration système requise de l'hôte.
- Vérifiez que la version 2.0 ou ultérieure du moteur d'exécution MSI est installée sur l'ordinateur hôte. Cette version du programme d'installation est disponible auprès de Microsoft pour les versions de Windows à partir de Windows XP. Consultez le site Web de Microsoft pour plus d'informations.

Procédure

1. Ouvrez une session sur le système hôte en tant qu'utilisateur administrateur ou en tant qu'utilisateur membre du groupe d'administrateurs local.

   Si vous ouvrez une session sur le domaine, le compte de domaine doit également être un administrateur local.

2. Extrayez l'image d'installation administrative à partir du fichier d'installation de Workstation Player.

   Le nom du fichier d'installation est semblable à `VMware-player-xxxx-xxxx.exe`, où *xxxx-xxxx* est la version et le numéro de build.

   Par exemple : **`setup.exe /s /e install_temp_path`**

3 Entrez la commande d'installation sur une ligne.

Ces exemples montrent les options que vous pouvez ajouter à la commande.

```
VMware-player-full-x.x.x-xxxxxx.exe /s /pass /v/qn REBOOT=ReallySuppress "EULAS_AGREED=1
INSTALLDIR=""path_to_program_directory"" ADDLOCAL=ALL SERIALNUMBER=""xxxxx-xxxxx-xxxxx-xxxxx-
xxxxx"" "
```

```
VMware-player-full-x.x.x-xxxxxx.exe /s /v/qn EULAS_AGREED=1 SERIALNUMBER="xxxxx-xxxxx-xxxxx-
xxxxx-xxxxx"
```

```
VMware-player-full-x.x.x-xxxxxx.exe /s /v/qn PLAYER_RVM_URI="vmware-
rvm://username@myserver.com:7443"
```

Vous pouvez utiliser la propriété `INSTALLDIR` facultative pour spécifier un chemin d'accès au fichier d'installation différent de l'emplacement par défaut.

REMARQUE Les guillemets autour du chemin d'accès au fichier sont importants. Tous les arguments MSI sont transmis avec l'option `/v`. Les guillemets extérieurs regroupent les arguments MSI et les guillemets intérieurs placent un guillemet dans cet argument.

Vous pouvez utiliser la propriété `REMOVE` facultative pour ignorer l'installation de certaines fonctionnalités.

Propriétés de l'installation sans assistance de Workstation Player

Lorsque vous exécutez une installation sans assistance de Workstation Player, vous pouvez personnaliser l'installation en spécifiant des propriétés d'installation dans la commande d'installation.

Pour spécifier une propriété d'installation dans la commande d'installation, utilisez le format `Property` = "*valeur*". La valeur 1 signifie true et la valeur 0 signifie false.

Tableau 2-1. Propriétés d'installation

Propriété	Description	Valeur par défaut
`AUTHD_PORT`	Spécifie à travers quel port communique le service d'autorisation VMware.	902
`AUTOSOFTWAREUPDATE`	Active les mises à niveau automatiques pour Workstation Player lorsqu'un nouveau build est disponible.	1
`DATACOLLECTION`	Envoie des informations sur l'expérience utilisateur à VMware.	1
`DESKTOP SHORTCUT`	Ajoute un raccourci sur le poste de travail lorsque Workstation Player est installé.	1
`EULAS_AGREED`	Vous permet d'accepter de manière silencieuse le CLUF du produit. Définissez-le sur 1 pour terminer l'installation ou la mise à niveau.	0
`INSTALL_DIR`	Installez Workstation Player dans un répertoire différent de l'emplacement par défaut de Workstation Player.	C:\Program Files (x86)\VMware\VMware Player
`KEEP_LICENSE`	Spécifie si les clés de licence sont conservées ou supprimées lorsque Workstation Player est installé.	1

Tableau 2-1. Propriétés d'installation (suite)

Propriété	Description	Valeur par défaut
KEEP_SETTINGFILES	Spécifie si les fichiers de paramètres sont conservés ou supprimés lorsque Workstation Player est désinstallé.	1
PLAYER_RVM_URI	Spécifie l'URI (Uniform Resource Identifier) du serveur Horizon FLEX Server.	VMware-player-full-x.x.x-xxxxxx.exe /s /v/qn PLAYER_RVM_URI="vmware-rvm://username@myserver.com:7443"
SERIALNUMBER	Vous permet d'entrer la clé de licence lorsque Workstation Player est installé. Entrez la clé de licence avec des traits d'union, par exemple xxxxx-xxxxx-xxxxx-xxxxx-xxxxx.	
SIMPLIFIEDUI	Active ou désactive certaines fonctions de l'interface utilisateur de Workstation Player.	0
SOFTWAREUPDATEURL	Spécifie une URL personnalisée pour la gestion des mises à jour logicielles (séparée de vmware.com).	
STARTMENU_SHORTCUT	Ajoute un élément au menu **Démarrer** lorsque Workstation Player est installé.	1
SUPPORTURL	Définit un alias d'URL ou d'e-mail de support spécifique que vos utilisateurs peuvent contacter pour faire part de problèmes sur les produits via le menu Workstation Player **Aide**.	

Configuration de certificats pour des machines virtuelles Horizon FLEX 3

Avant de créer et de déployer des machines virtuelles Horizon FLEX, vous devez configurer des certificats pour vous assurer que les utilisateurs finaux peuvent correctement télécharger et utiliser leurs machines virtuelles.

VMware vous recommande d'utiliser un certificat délivré par une autorité de certification, comme Entrust ou Go Daddy, ou un certificat tiers, sur votre Horizon FLEX Server. Si vous utilisez un certificat auto-signé ou un certificat d'une autorité de certification interne plutôt qu'un certificat généralement approuvé, vous devez suivre des étapes pour vous assurer que le certificat est approuvé sur tous les ordinateurs d'utilisateurs finaux qui téléchargeront et utiliseront des machines virtuelles Horizon FLEX.

Pour plus d'informations sur la configuration de certificats dans Mirage pour Horizon FLEX Server, consultez la documentation de Mirage à l'adresse https://www.vmware.com/support/pubs/mirage_pubs.html.

Ce chapitre aborde les rubriques suivantes :

Création d'une liste de certificats approuvés

Vous pouvez créer une liste de certificats approuvés pour des machines virtuelles Horizon FLEX et importer la liste dans le Serveur de stratégie Horizon FLEX. Lorsque vous utilisez une liste de certificats approuvés, vous n'avez pas à installer les certificats sur des hôtes d'utilisateurs finaux.

L'utilisation d'une liste de certificats approuvés peut empêcher les utilisateurs malintentionnés de créer leurs propres certificats auto-signés pour le même nom d'hôte et d'ajouter ces certificats à la liste de certificats approuvés de leur hôte.

Lorsque vous configurez le Serveur de stratégie Horizon FLEX pour utiliser une liste de certificats approuvés, l'hôte client ignore la liste de certificats de l'hôte et utilise la liste de certificats approuvés pour vérifier les connexions de serveur à la place. Si l'hôte client ne peut pas vérifier un certificat à l'aide de la liste de certificats approuvés, la connexion au serveur échoue.

Si la liste de certificats approuvés est vide dans la machine virtuelle source, Workstation Player et Fusion Pro s'authentifient avec la liste de certificats approuvés de l'hôte.

Pour créer la liste de certificats approuvés, vous exportez chaque certificat vers un fichier séparé, puis vous concaténez tous les fichiers en un seul fichier. Vous utilisez la Console d'administration Horizon FLEX pour importer le fichier de certificats concaténé dans le Serveur de stratégie Horizon FLEX.

Vous devez exporter les certificats au format PEM (Privacy Enhanced Mail). Sur les systèmes Windows, le codage de certificat PEM est appelé X.509 codé en Base64 (.cer). Seuls les certificats codés PEM sont pris en charge. Aucun autre format de certificat (DER, Serialized Certificate Store/SST, PKCS #12/PFX, PKCS #7/P7B) n'est accepté.

À propos du format PEM

Le format PEM est un format de certificat standard codé en Base64.

Voici un exemple de certificat au format PEM :

```
-----BEGIN CERTIFICATE-----
MIIDojCCAwugAwIBAgIJAMLM0CJRzPyzMA0GCSqGSIb3DQEBBQUAMIGTMQswCQYD
VQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTESMBAGA1UEBxMJUGFsbyBBbHRv
MS8wLQYDVQQKEyZWTXdhcmUsIEluYy4gLSBXb3Jrc3RhdGlvbiBTU0wgVGVzdGlu
ZzEqMCgGA1UEAxMhV29ya3N0YXRpb24gQ2VydGlmaWNhdGUgQXV0aG9yaXR5MB4X
DTExMDcxNTAyMjY0OFoXDTE1MDcxNDAyMjY0OFowgZMxCzAJBgNVBAYTAlVTMRMw
EQYDVQQIEwpDYWxpZm9ybmlhMRIwEAYDVQQHEwlQYWxvIEFsdG8xLzAtBgNVBAoT
JlZNd2FyZSwgSW5jLiAtIFdvcmtzdGF0aW9uIFNTTCBUZXN0aW5nMSowKAYDVQQD
EyFXb3Jrc3RhdGlvbiBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkwgZ8wDQYJKoZIhvcN
AQEBBQADgY0AMIGJAoGBAL/tBlngiEkCK7ssCBe8lZ30FlIHmpECmwEm3AaID1C0
lncb+LdRt2AmmQiknXBPxGBGyRNRNnashrzp1XXR/wL2b2AybT7NX+P/XSH2srDb
cGGCTNa/bwh/ArcirTLCjRwY55lAAH9xwzortRYR84IBJQpHzxcopTSI9o4ZVIqx
AgMBAAGjgfswgfgwHQYDVR0OBBYEFMoT527dtvlgR1EzYK4EnQHS6T2ZMIHIBgNV
HSMEgcAwgb2AFMoT527dtvlgR1EzYK4EnQHS6T2ZoYGZpIGWMIGTMQswCQYDVQQG
EwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTESMBAGA1UEBxMJUGFsbyBBbHRvMS8w
LQYDVQQKEyZWTXdhcmUsIEluYy4gLSBXb3Jrc3RhdGlvbiBTU0wgVGVzdGluZzEq
MCgGA1UEAxMhV29ya3N0YXRpb24gQ2VydGlmaWNhdGUgQXV0aG9yaXR5ggkAwszQ
IlHM/LMwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOBgQBcoiwDWGWXzI+j
0gG/7BNzpNHzR1RGAF4nB9JrnCYWvB313kgYDMHogfiAoQchsu/py/OYBYVRjjFJ
YVaTJ7DVl/3Gpk3+tcdJfEmqIz76PVWfWbTnhuJEMYrMM4W06B/K2cs24bkZtcXQ
h8b4FYTVCg/l6TP5SWgei4VWgRfxgA==
-----END CERTIFICATE-----
```

Lorsque vous créez une liste de certificats approuvés, vous concaténez plusieurs certificats au format PEM en un seul fichier. Les fins de lignes sont détectées automatiquement. L'exemple suivant indique le format d'une liste de certificats concaténés qui contient deux certificats.

```
-----BEGIN CERTIFICATE-----
<base64 content here>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<base64 content here>
-----END CERTIFICATE-----
```

Création de certificats au format PEM

Vous pouvez créer des certificats au format PEM en téléchargeant le certificat sur le site Web de l'autorité de certification ou en exportant les certificats à partir d'un système hôte.

Par exemple, vous pouvez télécharger des certificats pour Verisign sur le site Web de Symantec à l'adresse https://www.symantec.com/page.jsp?id=roots.

Exporter un certificat au format PEM depuis un Mac

Vous pouvez exporter un certificat au format PEM depuis un Mac.

Prérequis

Apprenez à utiliser Keychain Access sur un Mac. Pour plus d'informations, allez sur le site Web Assistance Apple à l'adresse http://support.apple.com.

Procédure

1 Sur le Mac, ouvrez Keychain Access.

2 Dans la barre latérale, sélectionnez **Racines du système**.

3 Localisez le certificat à exporter.

4 Sélectionnez **Fichier > Exporter des éléments**.

5 Sélectionnez un emplacement pour enregistrer le certificat et sélectionnez le format de fichier **Privacy Enhanced Mail (.pem)**.

Exporter un certificat au format PEM depuis un système Windows

Vous pouvez exporter un certificat au format PEM depuis un système Windows. Sous Windows, le codage de certificat PEM est appelé X.509 codé en Base64 (.cer).

Prérequis

Apprenez à utiliser le gestionnaire de certificats sur un système Windows. Pour plus d'informations, allez sur le site Web Microsoft TechNet à l'adresse http://technet.microsoft.com.

Procédure

1 Sur le système Windows, ouvrez le Gestionnaire de certificats (`certmgr.exe`).

2 Cliquez avec le bouton droit sur le certificat à exporter et sélectionnez **Toutes les tâches > Exporter**.

3 Sélectionnez des options dans l'Assistant Exportation de certificat.

   a Sélectionnez **X.509 codé en Base64 (.cer)** comme format d'exportation du fichier.

   Pour que le certificat fonctionne avec Horizon FLEX, vous devez choisir cette option.

   b Indiquez un emplacement pour enregistrer le certificat et un nom de fichier.

   c Examinez les paramètres que vous avez sélectionnés et cliquez sur **Terminer**.

   Le fichier de certificat est enregistré dans l'emplacement que vous avez indiqué.

Créer et importer le fichier de liste de certificats approuvés

Une fois que vous avez exporté vos certificats au format PEM, vous devez construire la liste de certificats approuvés et importer le fichier de liste de certificats dans le Serveur de stratégie Horizon FLEX.

Prérequis

Exportez chaque certificat au format PEM. Reportez-vous à « Création de certificats au format PEM », page 26.

Procédure

1 Pour créer le fichier de liste de certificats approuvés, concaténez chaque fichier de certificat au format PEM en un seul fichier.

Vous pouvez utiliser la commande `cat` ou copier et coller le contenu des fichiers de certificat dans un fichier texte. Vous pouvez modifier le contenu Base64 dans un éditeur de texte en toute sécurité.

Par exemple : `$ cat mycert1.pem mycert2.pem mycert3.pem > list.pem`

2 Démarrez la Console d'administration Horizon FLEX.

a Dans un navigateur Web, entrez **`https://WebManagerServer:7443/rvm`**, où *WebManagerServer* est le nom DNS ou l'adresse IP de l'hôte où Mirage Web Manager est installé.

b Entrez le nom d'utilisateur et le mot de passe d'un compte de domaine ayant accès à Mirage.

c Cliquez sur **Connexion**.

3 Dans la Console d'administration Horizon FLEX, cliquez sur l'icône **Paramètres système généraux** et sélectionnez **Certificats**.

4 Cliquez sur **Importer**, accédez au fichier de liste de certificats approuvés et cliquez sur **Ouvrir** pour importer le fichier.

Mise à jour des certificats sur le serveur

Lorsqu'un certificat expire et qu'un nouveau certificat a une date d'expiration éloignée, vous pouvez ajouter le nouveau certificat en tant que second certificat à la liste de certificats approuvés sur le Serveur de stratégie Horizon FLEX.

L'ajout du nouveau certificat à la liste de certificats approuvés permet à toutes les machines virtuelles Horizon FLEX de télécharger le nouveau certificat. Ensuite, lors du changement de certificat, toutes les machines virtuelles Horizon FLEX qui ont reçu la nouvelle liste de certificats peuvent se connecter au Horizon FLEX Server et vous pouvez supprimer l'ancien certificat approuvé du fichier de stratégie.

Si vous modifiez le certificat de serveur alors que les machines virtuelles Horizon FLEX ont déjà été enregistrées et exécutées, vos utilisateurs finaux doivent vérifier que le certificat modifié est approuvé par Fusion Pro ou Workstation Player. Si le nouveau certificat de serveur est auto-signé, le Horizon FLEX Client ne signale pas l'état de l'instance correctement à Horizon FLEX Server. L'utilisateur final doit ouvrir la machine virtuelle Horizon FLEX et cliquer sur **Se connecter** pour se connecter au serveur. Si l'utilisateur final reçoit le message d'erreur

`Certificat de sécurité non valide`

, l'utilisateur final doit voir avec vous si le certificat est valide et, si c'est le cas, cocher la case **Toujours faire confiance à cet hôte avec ce certificat** et cliquer sur **Se connecter quand même**.

Utilisation des certificats auto-signés

Si vous ne configurez pas le certificat auto-signé sur la machine virtuelle source préparée, vous devez installer le certificat sur chaque hôte d'utilisateur final pour que les machines virtuelles Horizon FLEX fonctionnent correctement.

Si la liste de certificats est vide dans le fichier de stratégie, Workstation Player et Fusion Pro ne parviennent pas à s'authentifier avec la liste de certificats approuvés de l'hôte.

Si vous incluez le certificat auto-signé d'une machine virtuelle source sur le Serveur de stratégie Horizon FLEX, et que vous configurez ou installez le certificat auto-signé pour le Horizon FLEX Client (dans le fichier de stratégie de la machine virtuelle source ou dans la liste de certificats approuvés de l'hôte), vous n'avez pas besoin d'installer le certificat sur les hôtes d'utilisateurs finaux lorsque des mises à jour de certificat sont requises, par exemple, lorsqu'un certificat expire.

Pour plus d'informations sur la configuration de certificats dans une machine virtuelle source, reportez-vous à « Créer une machine virtuelle source dans Fusion Pro », page 36.

Pour plus d'informations sur la création d'une liste de certificats approuvés et sur son importation sur le Serveur de stratégie Horizon FLEX, reportez-vous à « Création d'une liste de certificats approuvés », page 25.

Pour plus d'informations sur la mise à jour des certificats, reportez-vous à « Mise à jour des certificats sur le serveur », page 28.

Installer un certificat auto-signé sur un ordinateur Windows

Pour installer un certificat auto-signé sur un hôte Windows, vous exportez le certificat depuis votre Horizon FLEX Server et l'importez sur l'ordinateur Windows.

Prérequis

- Apprenez à installer et utiliser le composant logiciel enfichable Certificats MMC sur un système Windows. Pour plus d'informations, allez sur le site Web Windows TechNet à l'adresse http://technet.microsoft.com.
- Installez Windows IIS.

Procédure

1 Exportez le certificat auto-signé depuis votre serveur Horizon FLEX.

   a Sur le serveur Horizon FLEX, démarrez MMC (`mmc.exe`), ajoutez le composant logiciel enfichable Certificats pour un compte d'ordinateur, et gérez les certificats pour l'ordinateur local.

   b Sélectionnez **Fichier > Ajouter/Supprimer un composant logiciel enfichable**.

   c Cliquez sur le composant logiciel enfichable **Certificats** et cliquez sur **Ajouter**.

   d Dans la fenêtre **Composant logiciel enfichable Certificats**, sélectionnez **Compte d'ordinateur** et cliquez sur **Suivant**.

   Ce paramètre est requis par le serveur Horizon FLEX.

   e Sélectionnez **Ordinateur local** et cliquez sur **Terminer**, puis sur **OK**.

   f Dans le volet de navigation de gauche, développez **Certificats (ordinateur local)**.

   g Cliquez avec le bouton droit sur **Autorités de certification racines de confiance** et sélectionnez **Toutes les tâches > Importer**.

   L'Assistant Importation de certificat s'ouvre.

   h Cliquez sur **Suivant**.

   i Recherchez le fichier de certificat racine et cliquez sur **Suivant**.

   j Sélectionnez **Placer tous les certificats dans le magasin suivant : Autorités de certification racines de confiance** et cliquez sur **Suivant**, puis sur **Terminer**.

   k Cliquez avec le bouton droit sur **Autorités de certification racines intermédiaires** et sélectionnez **Toutes les tâches > Importer**.

   l L'**Assistant Importation de certificat** s'ouvre.

   m Recherchez le fichier de certificat racine et cliquez sur **Suivant**.

   n Sélectionnez **Placer tous les certificats dans le magasin suivant : Autorités de certification racines intermédiaires** et cliquez sur **Suivant**, puis sur **Terminer**.

   o Répétez les étapes m. et n. pour chaque certificat intermédiaire à installer.

p Accédez à **Autorités de certification racines de confiance > Certificats**.

q Sélectionnez et exportez le certificat auto-signé.

Exportez le certificat au format binaire codé DER X.509 (.cer).

2 Copiez le certificat auto-signé sur l'ordinateur Windows client.

3 Importez le certificat auto-signé sur l'ordinateur Windows client.

a Sur l'ordinateur Windows, démarrez MMC (`mmc.exe`).

b Ajoutez le composant logiciel enfichable Certificats pour le compte d'ordinateur et gérez les certificats pour l'ordinateur local.

c Importez le certificat auto-signé dans **Autorités de certification racines de confiance > Certificats**.

Le certificat auto-signé est maintenant approuvé pour tous les utilisateurs.

Installer un certificat auto-signé sur un Mac

Pour installer un certificat auto-signé sur un hôte Mac, vous exportez le certificat depuis votre Horizon FLEX Server et l'importez sur le Mac.

Prérequis

- Apprenez à installer et utiliser le composant logiciel enfichable Certificats MMC sur un système Windows. Pour plus d'informations, allez sur le site Web Windows TechNet à l'adresse http://technet.microsoft.com.
- Apprenez à utiliser Keychain Access sur un Mac. Pour plus d'informations, allez sur le site Web Assistance Apple à l'adresse http://support.apple.com.
- Installez Windows IIS.

Procédure

1 Exportez le certificat auto-signé depuis votre serveur Horizon FLEX.

a Sur le serveur Horizon FLEX, démarrez MMC (`mmc.exe`), ajoutez le composant logiciel enfichable Certificats pour un compte d'ordinateur, et gérez les certificats pour l'ordinateur local.

b Sélectionnez **Fichier > Ajouter/Supprimer un composant logiciel enfichable**.

c Cliquez sur le composant logiciel enfichable **Certificats** et cliquez sur **Ajouter**.

d Dans la fenêtre **Composant logiciel enfichable Certificats**, sélectionnez **Compte d'ordinateur** et cliquez sur **Suivant**.

Ce paramètre est requis par le serveur Horizon FLEX.

e Sélectionnez **Ordinateur local** et cliquez sur **Terminer**, puis sur **OK**.

f Dans le volet de navigation de gauche, développez **Certificats (ordinateur local)**.

g Cliquez avec le bouton droit sur **Autorités de certification racines de confiance** et sélectionnez **Toutes les tâches > Importer**.

L'Assistant Importation de certificat s'ouvre.

h Cliquez sur **Suivant**.

i Recherchez le fichier de certificat racine et cliquez sur **Suivant**.

j Sélectionnez **Placer tous les certificats dans le magasin suivant : Autorités de certification racines de confiance** et cliquez sur **Suivant**, puis sur **Terminer**.

k Cliquez avec le bouton droit sur **Autorités de certification racines intermédiaires** et sélectionnez **Toutes les tâches > Importer**.

l L'**Assistant Importation de certificat** s'ouvre.

m Recherchez le fichier de certificat racine et cliquez sur **Suivant**.

n Sélectionnez **Placer tous les certificats dans le magasin suivant : Autorités de certification racines intermédiaires** et cliquez sur **Suivant**, puis sur **Terminer**.

o Répétez les étapes m. et n. pour chaque certificat intermédiaire à installer.

p Accédez à **Autorités de certification racines de confiance > Certificats**.

q Sélectionnez et exportez le certificat auto-signé.

Exportez le certificat au format binaire codé DER X.509 (.cer).

2 Copiez le certificat auto-signé sur le Mac.

3 Importez le certificat auto-signé sur le Mac.

a Double-cliquez sur le certificat auto-signé pour l'ouvrir dans Keychain Access.

Le certificat auto-signé apparaît dans **Session**.

b Copiez le certificat auto-signé dans **Système**.

Vous devez copier le certificat dans **Système** pour vous assurer qu'il est approuvé par tous les utilisateurs et les processus système locaux, notamment les processus de machine virtuelle (vmware-vmx) dans Fusion Pro.

c Ouvrez le certificat auto-signé dans **Système**, développez **Se fier**, sélectionnez **Utiliser les réglages par défaut du système** et enregistrez vos modifications.

d Rouvrez le certificat auto-signé dans **Système**, développez **Approuver**, sélectionnez **Toujours approuver** et enregistrez vos modifications.

e Supprimez le certificat auto-signé de **Session**.

Utilisation de certificats d'autorité de certification internes

Si vous utilisez un certificat d'une autorité de certification interne au lieu d'une autorité de certification commerciale comme Entrust ou Go Daddy, et que vous ne configurez pas le certificat sur la machine virtuelle source préparée, vous devez installer le certificat d'autorité de certification racine sur l'hôte d'utilisateur final pour que les machines virtuelles Horizon FLEX fonctionnent correctement.

Remarque Comme le certificat de serveur est signé par l'autorité de certification racine, vous n'avez pas besoin d'importer le certificat de serveur sur les hôtes d'utilisateurs finaux.

Si la liste de certificats est vide dans le fichier de stratégie, Workstation Player et Fusion Pro ne parviennent pas à s'authentifier avec la liste de certificats approuvés de l'hôte.

Si vous incluez le certificat d'autorité de certification interne d'une machine virtuelle source sur le Serveur de stratégie Horizon FLEX, et que vous configurez ou installez le certificat pour le Horizon FLEX Client (dans le fichier de stratégie de la machine virtuelle source ou dans la liste de certificats approuvés de l'hôte), vous n'avez pas besoin d'installer le certificat d'autorité de certification racine sur les hôtes d'utilisateurs finaux lorsque des mises à jour de certificat sont requises, par exemple, lorsqu'un certificat expire.

Pour plus d'informations sur la configuration de certificats dans une machine virtuelle source, reportez-vous à « Créer une machine virtuelle source dans Fusion Pro », page 36.

Pour plus d'informations sur la création d'une liste de certificats approuvés et sur son importation sur le Serveur de stratégie Horizon FLEX, reportez-vous à « Création d'une liste de certificats approuvés », page 25.

Pour plus d'informations sur la mise à jour des certificats, reportez-vous à « Mise à jour des certificats sur le serveur », page 28.

Installer un certificat d'autorité de certification racine interne sur un ordinateur Windows

Pour installer un certificat d'autorité de certification racine interne sur un hôte Windows, vous exportez le certificat depuis votre serveur Horizon FLEX et l'importez sur l'ordinateur Windows.

Prérequis

- Apprenez à installer et utiliser le composant logiciel enfichable Certificats MMC sur un système Windows. Pour plus d'informations, allez sur le site Web Windows TechNet à l'adresse http://technet.microsoft.com.
- Obtenez et installez un certificat d'autorité de certification interne. Vous pouvez utiliser le composant logiciel enfichable Certificats MMC de Windows pour demander un certificat.
- Installez Windows IIS.

Procédure

1 Exportez le certificat d'autorité de certification racine depuis votre serveur Horizon FLEX.

   a Sur le serveur Horizon FLEX, démarrez MMC (`mmc.exe`), ajoutez le composant logiciel enfichable Certificats pour un compte d'ordinateur, et gérez les certificats pour l'ordinateur local.

   b Sélectionnez **Fichier > Ajouter/Supprimer un composant logiciel enfichable**.

   c Cliquez sur le composant logiciel enfichable **Certificats** et cliquez sur **Ajouter**.

   d Dans la fenêtre **Composant logiciel enfichable Certificats**, sélectionnez **Compte d'ordinateur** et cliquez sur **Suivant**.

   Ce paramètre est requis par Horizon FLEX Server.

   e Sélectionnez **Ordinateur local** et cliquez sur **Terminer**, puis sur **OK**.

   f Dans le volet de navigation de gauche, développez **Certificats (ordinateur local)**.

   g Cliquez avec le bouton droit sur **Autorités de certification racines de confiance** et sélectionnez **Toutes les tâches > Importer**.

   L'Assistant Importation de certificat s'ouvre.

   h Cliquez sur **Suivant**.

   i Recherchez le fichier de certificat racine et cliquez sur **Suivant**.

   j Sélectionnez **Placer tous les certificats dans le magasin suivant : Autorités de certification racines de confiance** et cliquez sur **Suivant**, puis sur **Terminer**.

   k Cliquez avec le bouton droit sur **Autorités de certification racines intermédiaires** et sélectionnez **Toutes les tâches > Importer**.

   l L'**Assistant Importation de certificat** s'ouvre.

   m Recherchez le fichier de certificat racine et cliquez sur **Suivant**.

   n Sélectionnez **Placer tous les certificats dans le magasin suivant : Autorités de certification racines intermédiaires** et cliquez sur **Suivant**, puis sur **Terminer**.

   o Répétez les étapes m. et n. pour chaque certificat intermédiaire à installer.

p Accédez à **Autorités de certification racines de confiance > Certificats**.

q Sélectionnez et exportez le certificat d'autorité de certification racine.

Exportez le certificat au format binaire codé DER X.509 (.cer).

2 Copiez le certificat d'autorité de certification racine sur l'ordinateur Windows.

3 Importez le certificat d'autorité de certification racine sur l'ordinateur Windows.

a Sur l'ordinateur Windows, démarrez MMC (`mmc.exe`).

b Ajoutez le composant logiciel enfichable Certificats pour le compte d'ordinateur et gérez les certificats pour l'ordinateur local.

c Importez le certificat d'autorité de certification racine dans **Autorités de certification racines de confiance > Certificats**.

Le certificat d'autorité de certification racine est maintenant approuvé pour tous les utilisateurs.

Installer un certificat d'autorité de certification racine interne sur un Mac

Pour installer un certificat d'autorité de certification racine interne sur un hôte Mac, vous exportez le certificat depuis votre Horizon FLEX Server et l'importez sur le Mac.

Prérequis

- Apprenez à installer et utiliser le composant logiciel enfichable Certificats MMC sur un système Windows. Pour plus d'informations, allez sur le site Web Windows TechNet à l'adresse http://technet.microsoft.com.
- Apprenez à utiliser Keychain Access sur un Mac. Pour plus d'informations, allez sur le site Web Assistance Apple à l'adresse http://support.apple.com.
- Installez Windows IIS.

Procédure

1 Exportez le certificat d'autorité de certification racine depuis votre serveur Horizon FLEX.

a Sur le serveur Horizon FLEX, démarrez MMC (`mmc.exe`), ajoutez le composant logiciel enfichable Certificats pour un compte d'ordinateur, et gérez les certificats pour l'ordinateur local.

b Sélectionnez **Fichier > Ajouter/Supprimer un composant logiciel enfichable**.

c Cliquez sur le composant logiciel enfichable **Certificats** et cliquez sur **Ajouter**.

d Dans la fenêtre **Composant logiciel enfichable Certificats**, sélectionnez **Compte d'ordinateur** et cliquez sur **Suivant**.

Ce paramètre est requis par Horizon FLEX Server.

e Sélectionnez **Ordinateur local** et cliquez sur **Terminer**, puis sur **OK**.

f Dans le volet de navigation de gauche, développez **Certificats (ordinateur local)**.

g Cliquez avec le bouton droit sur **Autorités de certification racines de confiance** et sélectionnez **Toutes les tâches > Importer**.

L'Assistant Importation de certificat s'ouvre.

h Cliquez sur **Suivant**.

i Recherchez le fichier de certificat racine et cliquez sur **Suivant**.

j Sélectionnez **Placer tous les certificats dans le magasin suivant : Autorités de certification racines de confiance** et cliquez sur **Suivant**, puis sur **Terminer**.

k Cliquez avec le bouton droit sur **Autorités de certification racines intermédiaires** et sélectionnez **Toutes les tâches > Importer**.

l L'**Assistant Importation de certificat** s'ouvre.

m Recherchez le fichier de certificat racine et cliquez sur **Suivant**.

n Sélectionnez **Placer tous les certificats dans le magasin suivant : Autorités de certification racines intermédiaires** et cliquez sur **Suivant**, puis sur **Terminer**.

o Répétez les étapes m. et n. pour chaque certificat intermédiaire à installer.

p Accédez à **Autorités de certification racines de confiance > Certificats**.

q Sélectionnez et exportez le certificat d'autorité de certification racine.

Exportez le certificat au format binaire codé DER X.509 (.cer).

2 Copiez le certificat d'autorité de certification racine sur le Mac.

3 Importez le certificat d'autorité de certification racine sur le Mac.

a Double-cliquez sur le certificat d'autorité de certification racine pour l'ouvrir dans Keychain Access.

Le certificat d'autorité de certification racine apparaît dans **Session**.

b Copiez le certificat d'autorité de certification racine dans **Système**.

Vous devez copier le certificat dans **Système** pour vous assurer qu'il est approuvé par tous les utilisateurs et les processus système locaux, notamment les processus de machine virtuelle (`.vmx`) dans Fusion.

c Ouvrez le certificat d'autorité de certification racine, développez **Approuver**, sélectionnez **Utiliser les réglages par défaut du système** et enregistrez vos modifications.

d Rouvrez le certificat d'autorité de certification racine, développez **Approuver**, sélectionnez **Toujours approuver** et enregistrez vos modifications.

e Supprimez le certificat d'autorité de certification racine de **Session**.

Création et déploiement de machines virtuelles Horizon FLEX 4

Vous pouvez créer plusieurs machines virtuelles Horizon FLEX et accorder des droits à ces machines virtuelles pour divers utilisateurs finaux, y compris des utilisateurs de Mac. Les utilisateurs peuvent être connectés ou déconnectés du réseau d'entreprise lorsqu'ils utilisent leurs machines virtuelles Horizon FLEX. Lorsque vous créez une machine virtuelle source pour une machine virtuelle Horizon FLEX, vous devez sélectionner certaines options pour que la machine virtuelle fonctionne correctement avec Horizon FLEX.

Vous pouvez utiliser Fusion Pro ou Workstation Pro (non inclus dans le package Horizon FLEX) pour créer une machine virtuelle source.

Ce chapitre aborde les rubriques suivantes :

Présentation du déploiement de machine virtuelle Horizon FLEX

Pour déployer une machine virtuelle Horizon FLEX, vous effectuez des tâches dans un ordre spécifique.

1 Créez et configurez une machine virtuelle source.

  Reportez-vous à « Créer une machine virtuelle source dans Fusion Pro », page 36 ou à « Créer une machine virtuelle source dans Workstation Pro (non inclus dans Horizon FLEX) », page 38.

2 (Facultatif) Préparez la machine virtuelle source à joindre à un domaine Active Directory.

  Reportez-vous à « Préparer une machine virtuelle source à joindre à un domaine Active Directory », page 40.

3 Comprimez le package de machine virtuelle source et enregistrez-le dans votre répertoire de téléchargement.

  Reportez-vous à « Comprimer un package de machine virtuelle source », page 41.

4 Enregistrez la machine virtuelle source avec le Serveur de stratégie Horizon FLEX.

Reportez-vous à « Enregistrer une machine virtuelle source avec le Serveur de stratégie Horizon FLEX », page 42.

5 Créez une stratégie pour l'image Horizon FLEX et accordez des droits pour l'image à vos utilisateurs et groupes Active Directory.

Reportez-vous à « Création de stratégies et de droits », page 43.

6 (Facultatif) Créez un URI pour déployer la machine virtuelle Horizon FLEX.

Reportez-vous à « Créer un URI pour déployer une machine virtuelle Horizon FLEX », page 51.

Créer une machine virtuelle source dans Fusion Pro

Vous pouvez utiliser Fusion Pro pour créer une machine virtuelle source pour une machine virtuelle Horizon FLEX. Lorsque vous créez une machine virtuelle source, vous devez définir des informations de cryptage et de restriction pour que la machine virtuelle fonctionne correctement avec Horizon FLEX.

Vous pouvez également utiliser Workstation Pro pour créer une machine virtuelle source. Workstation Pro n'est pas inclus dans le package Horizon FLEX.

Si vous activez l'utilisation des périphériques USB, le glisser-déposer et le copier-coller lorsque vous créez la machine virtuelle, vous pouvez définir des stratégies dans la Console d'administration Horizon FLEX pour activer ou désactiver ces fonctions pour les utilisateurs finaux. Toutefois, si vous désactivez ces fonctions lorsque vous créez la machine virtuelle, vous ne pouvez pas remplacer les paramètres de la machine virtuelle pour activer les fonctions en définissant des stratégies.

Horizon FLEX ne prend en charge que les noms de machine virtuelle utilisant des caractères anglais. N'utilisez pas de caractères non-ASCII dans les noms de fichier .vmx ou .tar. Fusion Pro ne peut pas créer des machines virtuelles Horizon FLEX en japonais ou en chinois simplifié.

Remarque Lorsque vous préparez une machine virtuelle Horizon FLEX, vérifiez que le fichier de stratégie .vmx se trouve dans le même dossier que tous les fichiers de disque de machine virtuelle (.vmdk). Si le fichier .vmx et les fichiers de disque de machine virtuelle se trouvent dans des répertoires différents sur la machine de l'utilisateur client, l'utilisateur reçoit un message d'erreur lorsqu'il tente de démarrer la machine virtuelle Horizon FLEX.

Prérequis

- Apprenez à créer une machine virtuelle dans Fusion Pro. Consultez la documentation de Fusion à l'adresse https://www.vmware.com/support/pubs/fusion_pubs.html.
- Découvrez les systèmes d'exploitation invités pris en charge pour les machines virtuelles Horizon FLEX. Reportez-vous à la section « Systèmes d'exploitation hôtes et invités pris en charge », page 12.
- Installez Fusion Pro avec une clé de licence Horizon FLEX.

Procédure

1 Ouvrez Fusion Pro et créez une machine virtuelle.

Sélectionnez un système d'exploitation invité pris en charge par les machines virtuelles Horizon FLEX. Lorsque la machine virtuelle est créée, Fusion Pro tente d'installer VMware Tools. Configurez la machine virtuelle pour distribution pour vos utilisateurs finaux.

2 Dans la bibliothèque de machines virtuelles, sélectionnez la nouvelle machine virtuelle et sélectionnez **Paramètres > Cryptage et restrictions**.

3 Sélectionnez **Activer le cryptage** et définissez un mot de passe pour ouvrir la machine virtuelle.

   Le mot de passe doit contenir au moins six caractères. Vous devez fournir ce mot de passe de cryptage à vos utilisateurs finaux pour qu'ils puissent ouvrir la machine virtuelle.

   Vous devez conserver le mot de passe de cryptage. Vous ne pouvez pas accéder à la machine virtuelle sans ce mot de passe.

4 Cochez **Activer les restrictions** et définissez un mot de passe pour modifier les restrictions sur la machine virtuelle.

   Ce mot de passe doit être différent du mot de passe de cryptage de la machine virtuelle.

   Vous devez conserver le mot de passe des restrictions. Il n'est pas possible de modifier les restrictions sur la machine virtuelle sans ce mot de passe.

5 Cliquez sur **Configurer**.

   La fenêtre de configuration des restrictions s'ouvre.

6 Définissez le **Type de restriction** sur **Géré**.

   Vous devez définir le type de restriction sur **Géré** pour distribuer et utiliser la machine virtuelle avec Horizon FLEX.

7 Saisissez l'URL du Horizon FLEX Server sur lequel vous voulez héberger la machine virtuelle dans la zone de texte **Serveur de gestion des restrictions**.

8 Cliquez sur **Vérifier le serveur** pour vérifier l'URL du Horizon FLEX Server.

9 (Facultatif) Pour ajouter des certificats approuvés à la machine virtuelle, cliquez sur le bouton **+** et accédez à l'emplacement de chaque fichier de certificat.

   Si vous ajoutez des certificats à la machine virtuelle, le Horizon FLEX Client utilise les certificats sur la machine virtuelle et n'utilise pas les certificats sur l'hôte. Pour procéder au contrôle et à la configuration de certificat sur le Serveur de stratégie Horizon FLEX pour toutes les machines virtuelles Horizon FLEX, laissez les cases des certificats vides.

10 Cliquez sur **Enregistrer**.

11 Cliquez sur l'icône **Verrou** pour empêcher toute modification ultérieure des restrictions de la machine virtuelle.

   Vous pouvez modifier les restrictions de la machine virtuelle en utilisant le mot de passe des restrictions.

Suivant

Si vous prévoyez de joindre la machine virtuelle Horizon FLEX à un domaine Active Directory, préparez la machine virtuelle à joindre au domaine. Reportez-vous à la section « Préparer une machine virtuelle source à joindre à un domaine Active Directory », page 40.

Pour installer le client Mirage dans la machine virtuelle source, reportez-vous à la section « Installer le Mirage Client sur une machine virtuelle source », page 39.

Créer une machine virtuelle source dans Workstation Pro (non inclus dans Horizon FLEX)

Vous pouvez utiliser Workstation Pro pour créer une machine virtuelle source pour une machine virtuelle Horizon FLEX. Workstation Pro n'est pas inclus dans le package Horizon FLEX. Une clé de licence Horizon FLEX pour Workstation Pro n'est pas requise.

Horizon FLEX ne prend en charge que les noms de machine virtuelle utilisant des caractères anglais. N'utilisez pas de caractères non-ASCII dans les noms de fichier .vmx ou .tar.

Remarque Lorsque vous préparez une machine virtuelle Horizon FLEX, vérifiez que le fichier de stratégie .vmx se trouve dans le même dossier que tous les fichiers de disque de machine virtuelle (.vmdk). Si le fichier .vmx et les fichiers de disque de machine virtuelle se trouvent dans des répertoires différents sur la machine de l'utilisateur client, l'utilisateur reçoit un message d'erreur lorsqu'il tente de démarrer la machine virtuelle Horizon FLEX.

Prérequis

- Revoyez comment créer une machine virtuelle dans Workstation Pro. Consultez la documentation de Workstation Pro à l'adresse https://www.vmware.com/support/pubs/ws_pubs.html
- Revoyez les systèmes d'exploitation invités pris en charge pour les machines virtuelles Horizon FLEX. Reportez-vous à « Systèmes d'exploitation hôtes et invités pris en charge », page 12.
- Installez Workstation.

Procédure

1. Ouvrez Workstation Pro et créez une machine virtuelle. Lorsque la machine virtuelle est créée, Workstation Pro tente d'installer VMware Tools.
2. Installez le système d'exploitation invité.

   Sélectionnez un système d'exploitation invité pris en charge par les machines virtuelles Horizon FLEX. Configurez la machine virtuelle pour distribution pour vos utilisateurs finaux.
3. Chiffrez et limitez la machine virtuelle. Sélectionnez la machine virtuelle et sélectionnez **VM > Paramètres**.
4. Dans l'onglet **Options**, sélectionnez **Contrôle d'accès**.
5. Cliquez sur **Chiffrer**, saisissez un mot de passe de chiffrement et cliquez sur **Chiffrer**.

   Le mot de passe de chiffrement est requis pour pouvoir accéder à la machine virtuelle. Il n'empêche pas l'utilisateur de modifier la configuration de la machine virtuelle. Activez les restrictions et entrez un mot de passe pour empêcher les utilisateurs de modifier la configuration de la machine virtuelle.

   Important Notez quelque part le mot de passe de chiffrement que vous utilisez. Si vous oubliez le mot de passe, Workstation ne fournit pas de moyen pour le récupérer.

   Workstation commence le chiffrement de la machine virtuelle. Une fois le processus de chiffrement terminé, vous pouvez définir un mot de passe des restrictions.
6. Cochez la case **Activer les restrictions** et définissez un mot de passe pour modifier les restrictions sur la machine virtuelle.

   Définissez un mot de passe différent du mot de passe de chiffrement de la machine virtuelle.

   Vous devez conserver le mot de passe des restrictions. Il n'est pas possible de modifier les restrictions sur la machine virtuelle sans ce mot de passe.

7 Définissez le **Type de restriction** sur **Géré**.

Vous devez définir le type de restriction sur **Géré** pour distribuer et utiliser la machine virtuelle avec Horizon FLEX.

8 Entrez l'URL d'Horizon FLEX Server sur lequel vous voulez héberger la machine virtuelle dans la zone de texte **Serveur de gestion des restrictions**.

9 Cliquez sur **Vérifier le serveur** pour vérifier l'URL du Horizon FLEX Server.

10 (Facultatif) Pour ajouter des certificats approuvés à la machine virtuelle, cliquez sur l'icône **Gérer les certificats** et accédez à l'emplacement de chaque fichier de certificat.

Si vous ajoutez des certificats à la machine virtuelle, le Horizon FLEX Client utilise les certificats sur la machine virtuelle et n'utilise pas les certificats sur l'hôte. Pour procéder au contrôle et à la configuration de certificat sur le Serveur de stratégie Horizon FLEX pour toutes les machines virtuelles Horizon FLEX, laissez les cases des certificats vides.

11 Cliquez sur **Enregistrer**.

Suivant

Si vous prévoyez de joindre la machine virtuelle Horizon FLEX à un domaine Active Directory, préparez la machine virtuelle à joindre au domaine. Reportez-vous à « Préparer une machine virtuelle source à joindre à un domaine Active Directory », page 40.

Pour installer le Mirage Client dans la machine virtuelle source, reportez-vous à « Installer le Mirage Client sur une machine virtuelle source », page 39.

Installer le Mirage Client sur une machine virtuelle source

Si la machine virtuelle source a un système d'exploitation invité Windows, vous pouvez installer le Mirage Client sur la machine virtuelle. L'installation du Mirage Client est facultative.

Si vous installez le client Mirage dans une machine virtuelle source, vous pouvez sélectionner des scénarios de reprise après sinistre lorsque vous autorisez la machine virtuelle. Par exemple, vous pouvez sélectionner une option pour que le serveur Mirage crée un CVD pour les machines virtuelles Horizon FLEX que l'utilisateur final télécharge. Mirage synchronise périodiquement les données de l'utilisateur dans le centre de données en fonction de la stratégie Mirage sélectionnée. Vous pouvez utiliser ces données pour restaurer le CVD ou accéder à des fichiers sur la machine virtuelle en utilisant le portail de fichier Mirage dans la console de gestion Mirage principale.

Remarque Lorsque vous configurez le serveur Mirage pour la récupération d'urgence, vérifiez que les ports MongoDB sont configurés correctement. Pour plus d'informations, consultez le *Guide d'installation de VMware Mirage*.

Prérequis

- Créez la machine virtuelle source. Reportez-vous à « Créer une machine virtuelle source dans Fusion Pro », page 36 ou à « Créer une machine virtuelle source dans Workstation Pro (non inclus dans Horizon FLEX) », page 38.
- Obtenez le *Guide d'installation de VMware Mirage* pour voir les instructions d'installation du client Mirage.

Procédure

1 Dans Fusion Pro ou Workstation Pro, démarrez la machine virtuelle source et ouvrez une session sur le système d'exploitation invité.

2 Installez la dernière version de VMware Tools.

   a Sur la barre de menus, sélectionnez **Machine virtuelle > Installer VMware Tools**.

   b Cliquez sur **Suivant** pour procéder à l'installation.

   c Sélectionnez **Terminer**, sauf si vous devez exclure certaines fonctionnalités de VMware Tools, puis cliquez sur **Suivant**.

   d Cliquez sur **Installer**.

   e Lorsque l'installation est terminée, cliquez sur **Oui** pour redémarrer la machine virtuelle.

3 Installez le client Mirage sur la machine virtuelle source.

   Consultez le *Guide d'installation de VMware Mirage* pour plus d'informations.

4 Dans la console de gestion Mirage, vérifiez que le point de terminaison apparaît avec l'état Affectation en attente.

   Remarque Ne supprimez pas cet enregistrement en attente tant que vous n'avez pas terminé la distribution de cette machine virtuelle source.

5 Dans la console de gestion Mirage, activez la création automatique de CVD.

   a Cliquez avec le bouton droit sur **Configuration système** et sélectionnez **Paramètres**.

   b Cliquez sur l'onglet **Création automatique de CVD**.

   c Sélectionnez **Activer la création automatique de CVD**.

   Vous pouvez modifier le message utilisateur si nécessaire.

   d Cliquez sur **OK**.

6 Mettez la machine virtuelle source hors tension dans Mirage lorsqu'elle présente l'état Affectation en attente.

   Ne fournissez pas le nom d'utilisateur et le mot de passe et n'enregistrez pas la machine virtuelle source à l'invite du client Mirage. Si vous enregistrez la machine virtuelle source avec Mirage, la machine virtuelle Horizon FLEX est dupliquée lorsque l'utilisateur y accède.

Une fois le client Mirage activé, lorsque vous créez un droit Horizon FLEX pour cette machine virtuelle source, les contrôles Mirage pour cette machine virtuelle sont disponibles.

Préparer une machine virtuelle source à joindre à un domaine Active Directory

Si vous prévoyez de joindre une machine virtuelle Horizon FLEX à un domaine Active Directory spécifique, vous devez préparer la machine virtuelle source à joindre au domaine avant de l'enregistrer avec le Serveur de stratégie Horizon FLEX.

Prérequis

- Créez une machine virtuelle source. Reportez-vous à « Créer une machine virtuelle source dans Fusion Pro », page 36 ou à « Créer une machine virtuelle source dans Workstation Pro (non inclus dans Horizon FLEX) », page 38.

  Remarque N'installez pas un système d'exploitation avec l'édition familiale de Windows 7 ou un système d'exploitation invité non-Windows sur la machine virtuelle source. Vous ne pouvez pas joindre un système d'exploitation avec l'édition familiale Windows 7 ou un système d'exploitation invité non-Windows à un domaine.

- Vérifiez que vous disposez du mot de passe administrateur de la machine virtuelle source.

- Dans la console d'administration Horizon FLEX, définissez la stratégie pour la machine virtuelle à joindre au domaine Active Directory. Le compte de l'administrateur d'Horizon FLEX doit avoir l'autorisation de créer des objets dans Active Directory.
- Un CDLS doit être installé dans la DMZ.
- Configurez Active Directory pour qu'il prenne en charge la jonction de domaine.

Procédure

1. Dans Fusion Pro, démarrez la machine virtuelle source et ouvrez une session sur le système d'exploitation invité.
2. (Facultatif) Désactivez **Windows Update**.
3. Installez la dernière version de VMware Tools.
   a. Sur la barre de menus, sélectionnez **Machine virtuelle > Installer VMware Tools**.
   b. Cliquez sur **Suivant** pour procéder à l'installation.
   c. Sélectionnez **Terminer**, sauf si vous devez exclure certaines fonctionnalités de VMware Tools, puis cliquez sur **Suivant**.
   d. Cliquez sur **Installer**.
   e. Lorsque l'installation est terminée, cliquez sur **Oui** pour redémarrer la machine virtuelle.
4. Exécutez `install-rvmsetup.cmd` en tant qu'administrateur pour installer VMware RVM Setup Service sur la machine virtuelle source.

   VMware RVM Setup Service exécute l'opération de jonction de domaine. `install-rvmsetup.cmd` est inclus avec VMware Tools.
5. Ouvrez le composant logiciel enfichable Windows Services (`services.msc`) et vérifiez que le type de démarrage de VMware RVM Setup Service est défini sur Automatique.
6. Arrêtez la machine virtuelle source.

   VMware RVM Setup Service démarre la prochaine fois que vous démarrez la machine virtuelle source.

Comprimer un package de machine virtuelle source

Vous devez comprimer le package de machine virtuelle source au format TAR (`.tar`) pour que les utilisateurs finaux puissent facilement télécharger la machine virtuelle. Un package de machine virtuelle (parfois appelé bundle) comporte tous les fichiers de machine virtuelle requis pour exécuter une machine virtuelle.

Prérequis

- Créez la machine virtuelle source. Reportez-vous à « Créer une machine virtuelle source dans Fusion Pro », page 36 ou à « Créer une machine virtuelle source dans Workstation Pro (non inclus dans Horizon FLEX) », page 38.
- Créez et configurez un dossier de téléchargement pour vos packages de machine virtuelle Horizon FLEX. Reportez-vous à « Créer un dossier de téléchargement pour des packages de machine virtuelle Horizon FLEX », page 17 et à « Configurer le certificat de serveur SSL IIS pour le Horizon FLEX Server », page 18.

Procédure

1. Si la machine virtuelle source est en cours d'exécution, arrêtez-la.
2. Dans Fusion Pro ou Workstation Pro, accédez à la machine virtuelle source.

3 Sélectionnez **Fichier > Exporter au format TAR** et exportez le package de machine virtuelle source vers un fichier TAR.

Supprimez tous les espaces du nom du fichier TAR. La suppression des espaces du nom de fichier peut faciliter la connexion à l'URL de téléchargement de la machine virtuelle.

4 Exportez le fichier TAR vers le dossier de téléchargement de vos packages de machine virtuelle Horizon FLEX.

Suivant

Enregistrez la machine virtuelle source avec le Serveur de stratégie Horizon FLEX. Reportez-vous à « Enregistrer une machine virtuelle source avec le Serveur de stratégie Horizon FLEX », page 42.

Enregistrer une machine virtuelle source avec le Serveur de stratégie Horizon FLEX

Vous devez enregistrer une machine virtuelle source avec le Serveur de stratégie Horizon FLEX sous forme d'image Horizon FLEX avant de pouvoir distribuer la machine virtuelle aux utilisateurs finaux.

Prérequis

- Comprimez les fichiers de la machine virtuelle source dans un fichier d'archive TAR (`.tar`). Reportez-vous à « Comprimer un package de machine virtuelle source », page 41.
- Vérifiez que le répertoire de téléchargement de vos packages de machine virtuelle Horizon FLEX est correctement configuré. Reportez-vous à « Créer un dossier de téléchargement pour des packages de machine virtuelle Horizon FLEX », page 17 et à « Configurer le certificat de serveur SSL IIS pour le Horizon FLEX Server », page 18.
- Vérifiez que des restrictions sont déjà définies dans le fichier de configuration (`.vmx`) de la machine virtuelle source. Si vous sélectionnez une machine virtuelle sans restrictions définies, le Serveur de stratégie Horizon FLEX rejette le fichier `.vmx` car non valide. Pour plus d'informations sur la définition des restrictions dans une machine virtuelle, reportez-vous à « Créer une machine virtuelle source dans Fusion Pro », page 36.

Procédure

1 Si la machine virtuelle source se trouve sur un Mac, effectuez ces étapes.

a Recherchez le fichier (`.vmwarevm`) du package de machine virtuelle de la machine virtuelle, cliquez avec le bouton droit sur le nom de fichier et sélectionnez **Afficher le contenu du package**.

b Copiez le fichier de configuration de la machine virtuelle (`.vmx`) dans un emplacement accessible au Horizon FLEX Server.

2 Démarrez la Console d'administration Horizon FLEX.

a Dans un navigateur Web, entrez **`https://`*`WebManagerServer`*`:7443/rvm`**, où *WebManagerServer* est le nom DNS ou l'adresse IP de l'hôte où Mirage Web Manager est installé.

b Entrez le nom d'utilisateur et le mot de passe d'un compte de domaine ayant accès à Mirage.

c Cliquez sur **Connexion**.

3 Cliquez sur **Images** dans le volet de navigation de gauche.

4 Cliquez sur le bouton **Nouveau** (+).

5 Cliquez sur **Sélectionner** à côté de la zone de texte **Sélectionner un fichier image** et accédez au fichier de configuration de la machine virtuelle (`.vmx`) de la machine virtuelle source.

6 Saisissez un nom convivial pour le fichier de machine virtuelle Horizon FLEX dans la zone de texte **Nom de l'image**.

Par exemple : `VM Windows 7`

7 (Facultatif) Saisissez une description de la machine virtuelle Horizon FLEX dans la zone de texte **Description**.

8 (Facultatif) Cliquez sur le bouton **Modifier** à côté de **Icône** et chargez une icône pour la machine virtuelle Horizon FLEX.

Les icônes chargées doivent être des fichiers PNG (`.png`).

9 (Facultatif) Dans la zone de texte **URL de l'image**, saisissez le chemin d'accès complet du fichier TAR qui contient le package de machine virtuelle source.

Les utilisateurs finaux téléchargent la machine virtuelle Horizon FLEX depuis cette URL. Le format de l'URL est `http://server:port/download_directory/filename.tar`, où *server* est le nom d'hôte ou l'adresse IP du serveur où vous avez stocké le fichier TAR, port est le numéro de port sur le serveur, *download_folder* est le nom du dossier de téléchargement de machine virtuelle Horizon FLEX qui contient le fichier TAR et *filename.tar* est le nom du fichier TAR qui contient le package de machine virtuelle source. L'URL peut commencer par http ou https.

Par exemple : `https://flexserver.demo.local:7443/flexdownloads/windows7vm.tar`

10 (Facultatif) Saisissez le texte dans la zone de texte **Clause de non-responsabilité (facultatif)**.

Si vous ne spécifiez aucun texte, le Horizon FLEX Client n'affiche pas de texte de clause de non-responsabilité lorsqu'un utilisateur télécharge la machine virtuelle Horizon FLEX.

11 Cliquez sur **OK** pour enregistrer la machine virtuelle source sous forme d'image Horizon FLEX.

12 (Facultatif) Saisissez l'URL de l'image dans un navigateur Web pour vérifier l'URL.

Par exemple : `https://flexserver.demo.local:7443/flexdownloads/windows7vm.tar`

Vous devez être invité à enregistrer le fichier. Si vous recevez une erreur liée aux autorisations, vous devrez peut-être ajuster les autorisations NTFS pour le dossier de téléchargement.

Suivant

Ajoutez des stratégies à l'image Horizon FLEX. Reportez-vous à « Configurer une stratégie générale pour une image Horizon FLEX », page 44.

Création de stratégies et de droits

Vous utilisez des stratégies pour définir une date d'expiration et pour contrôler les fonctions dans des instances de machine virtuelle créées à partir d'une image Horizon FLEX. Vous utilisez des droits pour que des utilisateurs et des groupes spécifiques puissent créer des instances de machine virtuelle à partir d'une image Horizon FLEX particulière.

Vous associez une stratégie à chaque droit que vous créez. Cette stratégie définit les paramètres de restriction par défaut des instances de machine virtuelle créées à partir de l'image Horizon FLEX dans le droit.

Vous pouvez inclure la même image Horizon FLEX dans plusieurs droits et vous pouvez associer chaque droit à une stratégie différente. Un même utilisateur peut être un membre de plusieurs droits.

Lorsqu'une instance de machine virtuelle est créée, les stratégies associées à des droits déterminent les restrictions initiales de l'instance. En tant qu'administrateur, vous pouvez modifier les paramètres de restriction d'une instance de machine virtuelle particulière. Les restrictions spécifiques des instances agissent comme restrictions pour une combinaison utilisateur/machine virtuelle spécifique. Pour plus d'informations sur la modification des restrictions de machines virtuelles, reportez-vous à « Gérer des machines virtuelles Horizon FLEX », page 53.

Configurer une stratégie générale pour une image Horizon FLEX

Vous configurez des stratégies générales pour définir une date d'expiration et pour contrôler les fonctions dans des instances de machine virtuelle créées à partir d'une image Horizon FLEX.

IMPORTANT Si les fonctions de copier-coller, de glisser-déposer et de partage de dossiers sont activées sur la machine virtuelle source, vous pouvez configurer une stratégie pour activer ou désactiver ces fonctions lorsque des utilisateurs téléchargent une instance de la machine virtuelle. Si ces fonctions sont désactivées sur la machine virtuelle source, vous ne pouvez pas remplacer les paramètres de la machine virtuelle en activant les fonctions dans une stratégie.

Vous sélectionnez la stratégie à affecter à une image Horizon FLEX lorsque vous accordez des droits pour l'image à des utilisateurs. Vous pouvez utiliser la même stratégie dans plusieurs droits.

Procédure

1 Démarrez la Console d'administration Horizon FLEX.

   a Dans un navigateur Web, entrez **`https://`*`WebManagerServer`*`:7443/rvm`**, où *WebManagerServer* est le nom DNS ou l'adresse IP de l'hôte où Mirage Web Manager est installé.

   b Entrez le nom d'utilisateur et le mot de passe d'un compte de domaine ayant accès à Mirage.

   c Cliquez sur **Connexion**.

2 Cliquez sur **Stratégies** dans le volet de navigation de gauche.

3 Cliquez sur l'onglet **Général** pour ajouter une stratégie ou sélectionnez une stratégie existante et cliquez sur **Modifier** pour la modifier.

4 Saisissez un nom pour la stratégie dans la zone de texte **Nom de stratégie**.

5 (Facultatif) Saisissez une description pour la stratégie dans la zone de texte **Description**.

6 Dans **Restrictions générales**, configurez les restrictions de la machine virtuelle.

Option	Action
Date d'expiration	Utilisez le widget calendrier pour définir une date d'expiration pour la machine virtuelle.
Opérations de copier-coller	Spécifiez si vous voulez autoriser les opérations de copier-coller dans la machine virtuelle. Cette stratégie contrôle les opérations de copier-coller entre l'invité et l'hôte de machine virtuelle. Elle ne contrôle pas les opérations de copier-coller dans la machine virtuelle.
Opérations de glisser-déposer	Spécifiez si vous voulez autoriser les opérations de glisser-déposer dans la machine virtuelle. Cette stratégie contrôle les opérations de glisser-déposer entre l'invité et l'hôte de machine virtuelle. Elle ne contrôle pas les opérations de glisser-déposer dans la machine virtuelle.
Paramètres du partage de dossiers	Spécifiez si vous voulez autoriser l'utilisation de dossiers partagés dans le système d'exploitation invité de machine virtuelle si l'administrateur a configuré des dossiers partagés dans la machine virtuelle.
Modifier les paramètres de mémoire et de CPU	Spécifiez si vous voulez autoriser les utilisateurs à modifier les paramètres de mémoire et de CPU de la machine virtuelle.
Demander à l'utilisateur de modifier la phrase de passe d'alimentation lorsqu'il déplace ou copie la machine virtuelle	Spécifiez si vous voulez que les utilisateurs modifient le mot de passe de cryptage s'ils déplacent ou copient la machine virtuelle.

Option	Action
Définir la phrase de passe de mise sous tension pour qu'elle corresponde à la phrase de passe AD de l'utilisateur après le premier démarrage	Spécifiez si le mot de passe que l'utilisateur entre lors de la mise sous tension de la machine virtuelle correspond au mot de passe Active Directory.
Interdire à l'utilisateur de créer plusieurs copies de la machine virtuelle	Spécifiez si vous voulez autoriser les utilisateurs à télécharger plusieurs instances de la machine virtuelle ou à copier des machines virtuelles déjà enregistrées.

7 (Facultatif) Dans **Messages pour les utilisateurs**, configurez les paramètres d'expiration de la machine virtuelle.

Le message par défaut est `Cette machine virtuelle est expirée.`

a Saisissez un message personnalisé supplémentaire à afficher à l'utilisateur lorsque la machine virtuelle est expirée.

b Cochez la case **Afficher ce message**, sélectionnez le nombre de jours avant l'expiration de la machine virtuelle pour afficher un message personnalisé et saisissez le texte de ce message.

8 Dans **Paramètres du serveur**, configurez les paramètres du serveur Horizon FLEX.

Option	Action
URL du serveur FLEX	Saisissez l'URL du serveur Horizon FLEX qui héberge le package de machine virtuelle. Ainsi : **`https://flexserver.demo.local:7443`** IMPORTANT N'ajoutez pas **`/rvm`** à la fin de l'URL.
Fréquence de contact du serveur	Sélectionnez la fréquence à laquelle la machine virtuelle contacte le serveur pour la synchronisation.
Limite de temps hors connexion	Définissez le nombre de jours pendant lesquels les utilisateurs peuvent utiliser la machine virtuelle avant qu'elle doive se connecter au serveur Horizon FLEX. Lorsque la limite de temps hors connexion est dépassée, la machine virtuelle doit se connecter au serveur Horizon FLEX pour pouvoir être mise sous tension.

9 Cliquez sur **OK** pour enregistrer la stratégie.

La nouvelle stratégie apparaît dans la liste de stratégies.

Suivant

Accordez des droits à la machine virtuelle Horizon FLEX. Reportez-vous à « Accorder des droits pour une image Horizon FLEX », page 48.

Configurer une stratégie de périphérique USB pour une image Horizon FLEX

Vous configurez des stratégies pour contrôler si des périphériques USB peuvent être utilisés sur des machines virtuelles créées à partir d'une image Horizon FLEX.

IMPORTANT Si le contrôleur de périphérique USB est présent sur la machine virtuelle source, vous pouvez configurer une stratégie pour activer ou désactiver cette fonction lorsque des utilisateurs téléchargent une instance de la machine virtuelle. Si cette fonction est désactivée sur la machine virtuelle source, vous ne pouvez pas remplacer les paramètres de la machine virtuelle en activant cette fonction dans une stratégie.

Procédure

1 Démarrez la Console d'administration Horizon FLEX.

   a Dans un navigateur Web, entrez **`https://WebManagerServer:7443/rvm`**, où *WebManagerServer* est le nom DNS ou l'adresse IP de l'hôte où Mirage Web Manager est installé.

   b Entrez le nom d'utilisateur et le mot de passe d'un compte de domaine ayant accès à Mirage.

   c Cliquez sur **Connexion**.

2 Cliquez sur **Stratégies** dans le volet de navigation de gauche.

3 Cliquez sur l'onglet **Contrôle de périphérique** pour ajouter une nouvelle stratégie de périphérique.

4 Sélectionnez le menu déroulant **Utilisation globale de périphériques USB** pour définir si la stratégie autorise ou bloque tous les périphériques USB sur la machine virtuelle.

   Toutes les classes de périphérique USB sont estompées et il n'est pas possible de les modifier. Reportez-vous à « Configurer une stratégie de périphérique USB personnalisée pour une image Horizon FLEX », page 46 pour créer une stratégie personnalisée dans laquelle des classes de périphérique USB spécifiques sont autorisées.

5 Cliquez sur **OK** pour enregistrer la stratégie.

   La nouvelle stratégie ou la stratégie mise à jour apparaît dans la liste de stratégies.

Suivant

Accordez des droits à la machine virtuelle Horizon FLEX. Reportez-vous à « Accorder des droits pour une image Horizon FLEX », page 48.

Configurer une stratégie de périphérique USB personnalisée pour une image Horizon FLEX

Vous pouvez configurer des stratégies de périphérique personnalisées pour contrôler si des types spécifiques de périphériques USB peuvent être utilisés sur des machines virtuelles créées à partir d'une image Horizon FLEX.

IMPORTANT Si le contrôleur de périphérique USB est présent sur la machine virtuelle source, vous pouvez configurer une stratégie pour activer ou désactiver cette fonction lorsque des utilisateurs téléchargent une instance de la machine virtuelle. Si cette fonction est désactivée sur la machine virtuelle source, vous ne pouvez pas remplacer les paramètres de la machine virtuelle en activant cette fonction dans une stratégie.

Procédure

1 Démarrez la Console d'administration Horizon FLEX.

   a Dans un navigateur Web, entrez **`https://WebManagerServer:7443/rvm`**, où *WebManagerServer* est le nom DNS ou l'adresse IP de l'hôte où Mirage Web Manager est installé.

   b Entrez le nom d'utilisateur et le mot de passe d'un compte de domaine ayant accès à Mirage.

   c Cliquez sur **Connexion**.

2 Cliquez sur **Stratégies** dans le volet de navigation de gauche.

3 Cliquez sur l'onglet **Contrôle de périphérique** pour ajouter une nouvelle stratégie de périphérique.

4 Définissez le menu déroulant **Utilisation globale de périphériques USB** sur **Personnalisé** pour autoriser ou bloquer des classes spécifiques de périphériques USB sur la machine virtuelle.

   Les zones de texte de la classe de périphériques USB apparaissent, ce qui vous permet d'autoriser ou de bloquer des classes spécifiques.

5 Sélectionnez les classes USB à autoriser ou à bloquer sur la machine virtuelle.

Tableau 4-1. Types de périphérique USB

Classe USB	Classe de base	Exemples
Audio	01h	Carte son USB
Périphérique de communication et CDC	02h	Adaptateur réseau USB, périphériques série RS-232
Physique	05h	Manette de jeu
Image	06h	Appareil photo USB, scanner USB, webcam
Imprimante	07h	Imprimante USB
Stockage de masse	08h	Disque USB
Carte à puce	0Bh	Lecteur de carte à puce USB
Sécurité du contenu	0Dh	Lecteur d'empreintes digitales
Vidéo	0Eh	Webcam
Contrôleur sans fil	E0h	Adaptateur Bluetooth, Microsoft RNDIS
Divers	EFh	Sélectionnez l'option **Divers** pour autoriser ou bloquer des périphériques USB non couverts dans les classes précédentes. Reportez-vous à Tableau 4-2 pour les classes USB qui requièrent le paramètre **Divers**.

Tableau 4-2. Classes de périphérique USB diverses

Classe USB	Classe de base	Exemples
Périphérique d'interface utilisateur	03h	Clavier USB, manette de jeu USB, souris USB
Concentrateur	09h	Concentrateur USB
Soins de santé	0Fh	Pulsomètre (montre)
Dispositif de diagnostic	DCh	Dispositif de test de conformité USB
Spécifique à l'application	FEh	Pont IrDA, classe d'essais et de mesures (USBTMC), Mise à niveau du microprogramme du périphérique USB (DFU)

6 Éventuellement, vous pouvez configurer la stratégie de périphérique pour autoriser des périphériques USB spécifiques.

a Sous la case **Autoriser la machine virtuelle à utiliser les périphériques USB suivants**, cliquez sur **Ajouter**.

b Entrez le nom du périphérique USB dans la zone de texte **Nom**.

c Entrez l'ID de fournisseur sous forme de valeur hexadécimale dans la zone de texte **ID de fournisseur**.

d Entrez l'ID de produit sous forme de valeur hexadécimale dans la zone de texte **ID de produit**.

e Cliquez sur **Ajouter** et sur **Mettre à jour**.

Pour obtenir les informations de périphérique USB sur une machine Windows, cliquez sur **Outils système**, puis sélectionnez **Gestionnaire de périphériques**. Pour obtenir des informations de périphérique USB sur un Mac, cliquez sur l'icône **Apple**, sélectionnez **À propos du Mac**, **Rapport système**, puis **USB** et cliquez sur le périphérique.

7 Cliquez sur **OK** pour enregistrer la stratégie.

La nouvelle stratégie ou la stratégie mise à jour apparaît dans la liste de stratégies.

Suivant

Accordez des droits à la machine virtuelle Horizon FLEX. Reportez-vous à « Accorder des droits pour une image Horizon FLEX », page 48.

Mettre à jour une stratégie pour une image Horizon FLEX déployée

Après le déploiement d'une image Horizon FLEX pour des utilisateurs, vous pouvez mettre à jour des stratégies qui s'appliquent à des instances de machine virtuelle existantes.

IMPORTANT Si vous modifiez une stratégie existante à l'aide du bouton **Stratégies** dans le volet de navigation de gauche, la modification ne s'applique qu'aux nouveaux utilisateurs. La stratégie modifiée ne s'applique pas aux utilisateurs existants avec des instances de machine virtuelle déployées. Par exemple, dans un scénario où la stratégie d'origine n'empêche pas l'utilisateur de créer plusieurs copies de la machine virtuelle, si vous modifiez la stratégie pour ajouter cette restriction, elle ne s'appliquerait pas aux machines virtuelles existantes. Si un utilisateur dispose d'une machine virtuelle couverte par la stratégie d'origine, cet utilisateur peut toujours faire des copies de cette machine virtuelle. Si cet utilisateur télécharge une deuxième machine virtuelle couverte par la stratégie modifiée, l'utilisateur ne pourrait pas copier cette deuxième machine virtuelle.

Procédure

1 Démarrez la Console d'administration Horizon FLEX.

   a Dans un navigateur Web, entrez **`https://WebManagerServer:7443/rvm`**, où *WebManagerServer* est le nom DNS ou l'adresse IP de l'hôte où Mirage Web Manager est installé.

   b Entrez le nom d'utilisateur et le mot de passe d'un compte de domaine ayant accès à Mirage.

   c Cliquez sur **Connexion**.

2 Cliquez sur **Machines virtuelles** dans le volet de navigation de gauche.

3 Sélectionnez la machine virtuelle.

4 Cliquez sur **Modifier**.

5 Mettez à jour la stratégie de la machine virtuelle et cliquez sur **OK** lorsque vous avez terminé.

Suivant

Reportez-vous à la section « Configurer une stratégie générale pour une image Horizon FLEX », page 44 et « Configurer une stratégie de périphérique USB pour une image Horizon FLEX », page 45 pour plus d'informations.

Accorder des droits pour une image Horizon FLEX

Vous utilisez des droits pour autoriser des utilisateurs et des groupes spécifiques à télécharger et utiliser des instances de machine virtuelle à partir d'une image Horizon FLEX particulière.

Les utilisateurs peuvent télécharger n'importe quelle machine virtuelle Horizon FLEX pour lesquelles ils ont des droits. Les utilisateurs doivent entrer leurs informations d'identification Active Directory avant de pouvoir enregistrer et utiliser une machine virtuelle Horizon FLEX pour la première fois. Les utilisateurs peuvent ouvrir une session sur le serveur Horizon FLEX et télécharger la machine virtuelle. Ils peuvent également copier la machine virtuelle Horizon FLEX depuis un périphérique USB et entrer les informations d'identification Active Directory lors du premier démarrage de la machine virtuelle.

Prérequis

- Vérifiez que les utilisateurs et les groupes Active Directory appropriés sont synchronisés dans la base de données Horizon FLEX. Reportez-vous à « Configurer les paramètres Active Directory », page 19.
- Enregistrez la machine virtuelle source avec le Serveur de stratégie Horizon FLEX. Reportez-vous à « Enregistrer une machine virtuelle source avec le Serveur de stratégie Horizon FLEX », page 42.
- Configurez une stratégie pour l'image Horizon FLEX. Reportez-vous à « Configurer une stratégie générale pour une image Horizon FLEX », page 44.

Procédure

1 Démarrez la Console d'administration Horizon FLEX.

   a Dans un navigateur Web, entrez `https://WebManagerServer:7443/rvm`, où *WebManagerServer* est le nom DNS ou l'adresse IP de l'hôte où Mirage Web Manager est installé.

   b Entrez le nom d'utilisateur et le mot de passe d'un compte de domaine ayant accès à Mirage.

   c Cliquez sur **Connexion**.

2 Cliquez sur **Droits** dans le volet de gauche.

3 Cliquez sur le bouton **Nouveau** (+) pour créer un droit, sélectionnez un droit existant et cliquez sur **Modifier** pour le modifier ou sélectionnez un droit existant et cliquez sur **Dupliquer** pour le dupliquer.

4 Créez le nom de droit et attribuez-le à une image Horizon FLEX.

   a Entrez un nom pour le droit dans la zone de texte **Nom de droit**.

   b Sélectionnez une image Horizon FLEX à ajouter au droit.

   Vous pouvez utiliser le champ de recherche pour filtrer la liste d'images Horizon FLEX.

   Si vous dupliquez un droit existant, vous devez le renommer avant de l'enregistrer.

   Lorsque vous sélectionnez l'image Horizon FLEX, l'URL de téléchargement de l'image est automatiquement renseignée dans la zone de texte **URL de téléchargement**.

   c Dans la zone de texte **URL de téléchargement**, entrez l'URL que le client utilise pour télécharger l'image Horizon FLEX.

   d Cliquez sur **Suivant**.

5 Sélectionnez les utilisateurs et groupes Active Directory à inclure dans le droit.

   a Utilisez le champ de recherche pour rechercher et sélectionner les utilisateurs et les groupes à ajouter au droit.

   15 minutes peuvent être nécessaires avant que les nouveaux utilisateurs et groupes Active Directory apparaissent dans les résultats de la recherche.

   b Cliquez sur **Ajouter** pour ajouter un utilisateur ou un groupe à la liste Membres des droits.

   Vous pouvez utiliser les boutons **Supprimer** ou **Effacer tout** pour gérer la liste de membres.

   c Cliquez sur **Suivant**.

6 Sélectionnez une stratégie pour le droit et cliquez sur **Suivant**.

   Vous pouvez utiliser le champ de recherche pour filtrer la liste de stratégies et les boutons **Effacer le filtre** et **Afficher le filtre** pour gérer vos recherches.

7 (Facultatif) Pour utiliser un modèle d'attribution de nom de machine virtuelle, sélectionnez **Utiliser la configuration de nom de machine** et configurez le modèle d'attribution de nom.

a Entrez le modèle d'attribution de nom de machine à utiliser dans la zone de texte **Modèle d'attribution de nom de machine**.

Pour vous assurer que chaque machine virtuelle reçoit un nom différent et peut joindre le domaine, incluez l'espace réservé {*username*}. Cet espace réservé est remplacé par le nom de l'utilisateur lorsque ce dernier télécharge la machine virtuelle. Vous pouvez également créer un modèle de numéro à l'aide de l'espace réservé {*n*} afin d'incrémenter des numéros de machine virtuelle avec des noms d'utilisateur.

Pour plus d'informations, consultez « Créer un modèle d'attribution de nom de machine virtuelle », page 51.

b Sélectionnez un nom de domaine dans le menu déroulant **Nom de domaine**.

c Entrez une unité d'organisation dans la zone de texte **Unité d'organisation**.

Par exemple : `OU=hr1, OU=hr, OU=flex, DC=ws, DC=test, DC=com`

8 (Facultatif) Si vous avez installé le Mirage Client sur la machine virtuelle, choisissez de gérer la machine virtuelle avec Mirage.

Option	Description
Utiliser VMware Mirage dans des scénarios de reprise après sinistre et de gestion d'images	Sélectionnez cette option pour choisir une stratégie de CVD, une couche de base, une couche d'application et d'autres configurations. Le Mirage Server crée automatiquement un CVD pour les machines virtuelles que l'utilisateur télécharge. Mirage synchronise périodiquement les données de l'utilisateur final dans le centre de données en fonction de la stratégie Mirage sélectionnée. Dans la console de gestion Mirage principale, vous pouvez utiliser ces données pour restaurer le CVD ou accéder à des fichiers sur la machine virtuelle en utilisant le portail de fichier Mirage. Le Mirage Server déploie également automatiquement les couches de base et d'application sur la machine virtuelle après son provisionnement pour la conformité des images et la remise des applications distantes.
Utiliser VMware Mirage dans des scénarios de reprise après sinistre	Sélectionnez cette option pour choisir une stratégie de CVD. Le Mirage Server crée un CVD pour les machines virtuelles que l'utilisateur final télécharge. Vous pouvez utiliser ces données pour restaurer le CVD ou accéder à des fichiers sur la machine virtuelle en utilisant le portail de fichier Mirage dans la console de gestion Mirage principale.
Ne pas utiliser VMware Mirage pour gérer les machines virtuelles	Sélectionnez cette option pour désactiver la gestion de la machine virtuelle avec Mirage.

Si vous supprimez une machine virtuelle dans laquelle le Mirage Client est installé, le Mirage Server archive le CVD de la machine virtuelle supprimée.

9 Cliquez sur **Suivant** et examinez les paramètres du droit.

10 Cliquez sur **Terminer** pour enregistrer le droit ou cliquez sur **Précédent** pour revenir à la page précédente et modifier le droit.

Créer un modèle d'attribution de nom de machine virtuelle

Lorsque vous accordez des droits pour une image Horizon FLEX, vous pouvez créer un modèle d'attribution de nom de machine virtuelle afin que, quand des machines virtuelles sont créées pour le même droit d'utilisateur, Horizon FLEX crée des noms de machine virtuelle uniques.

Le modèle d'attribution de nom de machine virtuelle doit inclure les paramètres {*username*} ou {*n*}. Le paramètre {*n*} permet de créer un modèle de numéro afin d'ajouter des incrémentations aux noms de machine virtuelle. Ces modèles sont valides :

- VM-{*username*}
- VM-{*n*}

Ces modèles ne sont pas valides :

- VM-(*username*}-{*username*}
- VM-{*username*}-{*n*}
- VM-{*n*}-{*n*}

Le nom de machine peut contenir 15 caractères au maximum. Si un nom de machine contient plus de 15 caractères, seuls les 15 premiers caractères sont utilisés. Par exemple, si le modèle est VM-1234567890-*username* et que le nom d'utilisateur est Jack, le nom de machine est tronqué et devient VM-1234567890-J.

Pour vous assurer que chaque machine virtuelle reçoit un nom différent et peut joindre le domaine, le nom doit inclure les espaces réservés {*username*} ou {*n*}. L'espace réservé {*username*} est remplacé par le nom de l'utilisateur lorsque ce dernier télécharge la machine virtuelle. Pour {*n*}, les ordinateurs dont le nom correspond au modèle sont recherchés dans Active Directory. Si aucun nom ne correspond au modèle, le numéro est 1. Sinon, la valeur du numéro suivant est le numéro qui suit le numéro maximal parmi tous les noms qui correspondent au modèle.

Par exemple, une machine virtuelle peut être accordée à user1 et le modèle d'attribution de nom de machine peut être défini sur VM-*username- n*. Lorsque user1 télécharge la machine virtuelle, une recherche est effectuée dans Active Directory pour déterminer si un nom de machine correspond au modèle d'attribution de nom, tel que VM-user1-*x*, où *x* est le numéro attribué. Si le numéro de mappage maximal est 25, où le nom de machine virtuelle est VM-user1-25, cette machine est nommée VM-user1-26. Si aucune machine virtuelle ne correspond au modèle, Horizon FLEX nomme la machine VM-user1-1.

Vous pouvez accorder plusieurs machines virtuelles au même utilisateur. Par exemple, vous pouvez accorder trois machines virtuelles à user1. Lorsque user1 télécharge les machines virtuelles, le nom de machine virtuelle devient vm-*x*-user1. Le numéro de machine virtuelle attribué n'est pas incrémenté pour chaque nom d'utilisateur, mais il est basé sur la date d'enregistrement de la machine virtuelle.

Par exemple, user1 peut avoir trois noms de machine virtuelle vm-10-user1, vm-26-user1 et vm-39-user1, en fonction des autres machines virtuelles qui ont été accordées à d'autres utilisateurs et en fonction du moment où user1 a téléchargé chaque machine virtuelle. Le numéro incrémenté est utilisé uniquement à des fins de suivi par l'administrateur d'Horizon FLEX. L'utilisateur client ne voit pas le numéro incrémenté.

Créer un URI pour déployer une machine virtuelle Horizon FLEX

Vous pouvez déployer une machine virtuelle Horizon FLEX en créant un URI (Uniform Resource Identifier). Avec un URI, vous pouvez créer un e-mail qui contient un lien sur lequel l'utilisateur final peut cliquer pour se connecter à un serveur et télécharger une machine virtuelle Horizon FLEX.

Prérequis

- Vérifiez que le Horizon FLEX Client est installé sur le système d'utilisateur final.
- Donnez à l'utilisateur final un mot de passe pour le serveur et un mot de passe de chiffrement pour la machine virtuelle.

Procédure

1 Construisez un URI pour l'utilisateur.

Un URI a la structure suivante :

`vmware-rvm://username@myserver.com:7443`

username est le nom de connexion de l'utilisateur et *myserver.com* est le nom d'hôte du serveur. Vous devez inclure `vmware-rvm://` et `:7443` dans l'adresse du serveur. N'incluez pas http ou https dans l'adresse du serveur.

2 Saisissez le texte du lien dans un e-mail et entrez les informations sur le lien hypertexte pour l'URI.

Vous pouvez utiliser n'importe quel système de messagerie pour envoyer le lien. Toutefois, comme le format de l'URI n'est pas reconnu comme une URL standard, vous devez entrer manuellement les informations sur le lien hypertexte.

3 Créez un e-mail pour l'utilisateur et entrez le texte du lien.

Par exemple : **`Votre machine virtuelle Horizon FLEX`**

4 Sélectionnez le texte du lien, cliquez dessus avec le bouton droit et sélectionnez **Lien hypertexte**.

5 Sélectionnez **Lien vers : Fichier ou page Web existant(e)**.

6 Entrez l'URI dans la zone de texte **Adresse**.

Par exemple : **`vmware-rvm://johndoe@yourserver.com:7443`**

Le lien est maintenant actif.

7 Cliquez sur **OK**.

8 Envoyez l'e-mail à l'utilisateur.

Lorsque l'utilisateur clique sur le lien dans l'e-mail, le Horizon FLEX Client de l'utilisateur démarre et la boîte de dialogue de connexion au serveur s'ouvre. Les cases du serveur et du nom d'utilisateur sont pré-remplies avec les valeurs que vous avez spécifiées dans l'URI. L'utilisateur entre un mot de passe et se connecte au serveur pour télécharger une machine virtuelle.

Gestion de machines virtuelles Horizon FLEX 5

Vous pouvez gérer des machines virtuelles Horizon FLEX déployées en exécutant des opérations telles que Modifier, Verrouiller, Réactiver, Effacer, Archiver ou Supprimer.

Gérer des machines virtuelles Horizon FLEX

Une fois les machines virtuelles Horizon FLEX déployées, vous pouvez les gérer en exécutant différentes opérations. Vous pouvez voir l'inventaire de machines virtuelles Horizon FLEX déployées dans la Console d'administration Horizon FLEX.

Vous pouvez utiliser la zone de texte **Rechercher** pour filtrer la liste de machines virtuelles et les en-têtes de colonne triables pour trouver une machine virtuelle spécifique. Utilisez le menu déroulant des en-têtes de colonne pour sélectionner les colonnes que vous voulez afficher ou masquer.

Lorsque vous sélectionnez une machine virtuelle dans la liste, vous pouvez agrandir la fenêtre Propriétés en bas de la page pour voir des paramètres généraux de la machine virtuelle, ainsi que des stratégies qui y sont appliquées.

Procédure

1 Démarrez la Console d'administration Horizon FLEX.

   a Dans un navigateur Web, entrez **`https://WebManagerServer:7443/rvm`**, où *WebManagerServer* est le nom DNS ou l'adresse IP de l'hôte où Mirage Web Manager est installé.

   b Entrez le nom d'utilisateur et le mot de passe d'un compte de domaine ayant accès à Mirage.

   c Cliquez sur **Connexion**.

2 Cliquez sur **Machines virtuelles** dans le volet de navigation de gauche.

   L'inventaire de machines virtuelles Horizon FLEX déployées apparaît sur la page Machines virtuelles.

3 Pour gérer une machine virtuelle spécifique, sélectionnez-la dans la liste.

Option	Action
Modifier	Sélectionnez une machine virtuelle et cliquez sur **Modifier** pour modifier les stratégies affectées à cette machine virtuelle.
Verrouillage	Sélectionnez une machine virtuelle et cliquez sur **Verrouillage** pour révoquer l'accès utilisateur à la machine virtuelle spécifique.
Réactiver	Sélectionnez une machine virtuelle expirée ou verrouillée et cliquez sur **Réactiver** pour réinitialiser la machine virtuelle.
Effacer	Sélectionnez une machine virtuelle et cliquez sur **Effacer** pour la supprimer du système de fichiers.

Option	Action
Archive	Sélectionnez une machine virtuelle et cliquez sur **Archive** pour désactiver la machine virtuelle et conserver un enregistrement hors connexion de la machine virtuelle. Cochez la case **Afficher les instances archivées** en bas de la page Machines virtuelles pour voir les machines virtuelles qui ont été archivées. Vous pouvez cliquer sur **Réactiver** pour activer une machine virtuelle archivée.
Supprimer	Sélectionnez une machine virtuelle archivée et cliquez sur **Supprimer**. Vous ne pouvez pas supprimer une machine virtuelle avec un statut qui n'est pas Archivé.

4 Pour déterminer les actions possibles pour une machine virtuelle, affichez son état dans la colonne État.

État	Description
Active	La machine virtuelle est utilisée, a contacté le serveur et n'a pas expiré.
Inactive	Le Horizon FLEX Client que l'utilisateur a utilisé pour ouvrir la machine virtuelle n'est pas parvenu à contacter le serveur au-delà de la période de stratégie de travail hors connexion.
Expirée	La date d'expiration a été atteinte et la machine virtuelle a été mise hors tension.
Expirée en attente	Le serveur attend la confirmation du Horizon FLEX Client que la machine virtuelle est expirée.
Verrouillée	Un administrateur a verrouillé l'utilisateur de la machine virtuelle.
Verrouillage en attente	Un verrouillage a été initié. L'état reste En attente jusqu'à ce que le Horizon FLEX Client vérifie que la machine virtuelle a été verrouillée.
Réactivation en attente	Le serveur attend la confirmation du Horizon FLEX Client que la machine virtuelle est réactivée.
Téléchargement	L'utilisateur télécharge la machine virtuelle.
Téléchargement annulé	L'utilisateur a annulé le téléchargement.
Téléchargement suspendu	L'utilisateur a suspendu le téléchargement.
Échec de jonction du domaine	La machine virtuelle n'est pas parvenue à joindre un domaine. La raison la plus courante pour laquelle une machine virtuelle ne parvient pas à joindre un domaine est que l'objet existe déjà dans Active Directory. Dans ce cas, consultez le journal de jonction du domaine hors connexion, géré par le système d'exploitation, pour déterminer comment résoudre l'échec.
Supprimé par l'utilisateur	L'utilisateur a supprimé la VM sur le client.
Effacé	La machine virtuelle a été effacée par l'administrateur et supprimée du système de l'utilisateur.
Effacement en attente	Le serveur attend la confirmation d'Horizon FLEX Client que la machine virtuelle a été supprimée du système de l'utilisateur.
Archivée	La machine virtuelle a été archivée. **Remarque** Vous devez cocher la case **Afficher les instances archivées** pour voir les machines virtuelles archivées.

Maintenance du système Horizon FLEX 6

Vous pouvez exécuter des opérations de maintenance sur le système Horizon FLEX, y compris la mise à niveau depuis des versions précédentes d'Horizon FLEX.

Ce chapitre aborde les rubriques suivantes :

Mettre à niveau à partir de versions précédentes d'Horizon FLEX

Vous pouvez mettre à niveau le système Horizon FLEX à partir de versions précédentes d'Horizon FLEX.

Prérequis

- Tous les serveurs Mirage sont arrêtés.
- Toutes les machines virtuelles Horizon FLEX déployées sont arrêtées.

Procédure

1 Téléchargez les fichiers d'installation d'Horizon FLEX Server et d'Horizon FLEX Client pour la version de mise à niveau.

2 Mettez à niveau le composant Horizon FLEX Server.

   a Pour mettre à niveau le serveur de gestion Mirage, double-cliquez sur le fichier mirage.management.server.64x.*buildnumber*.msi dans le dossier du serveur.

   Par défaut, les paramètres de configuration que vous avez sélectionnés pendant l'installation initiale sont appliqués. Vous pouvez modifier les paramètres de configuration pendant le processus de mise à niveau.

   b Pour mettre à niveau le serveur Mirage, double-cliquez sur le fichier mirage.server.64x.*buildnumber*.msi.

   Par défaut, les paramètres de configuration que vous avez sélectionnés pendant l'installation initiale sont appliqués. Vous pouvez modifier les paramètres de configuration pendant le processus de mise à niveau.

   c Pour mettre à niveau Mirage Web Manager (console de gestion Web), double-cliquez sur le fichier mirage.WebManagement.console.x64.*buildnumber*.msi dans le dossier WebManagement.

   Continuez sans apporter de modification.

   d Si vous utilisez Mirage pour gérer vos machines virtuelles Windows, suivez les instructions de mise à niveau depuis la version précédente de Mirage dans le *Guide de l'administrateur de VMware Mirage*.

3 Mettez à niveau tous les clients Horizon FLEX vers la version compatible avec le Horizon FLEX Server mis à niveau.

- Fournissez aux utilisateurs le fichier d'installation pour la version de mise à niveau de Fusion Pro ou de Workstation Player, ou demandez-leur de télécharger le logiciel sur le site Web de VMware.
- Mettez à niveau les clients Horizon FLEX Client en utilisant un déploiement en masse.

Suivant

Pour des instructions complètes sur la mise à niveau de Mirage, consultez la documentation de VMware Mirage à l'adresse https://www.vmware.com/support/pubs/mirage_pubs.html.

Remarque Ne sélectionnez pas **Créer de nouvelles zones de stockage** lors de la mise à niveau de Mirage Management Server. Si vous sélectionnez cette option et entrez le chemin d'accès à la zone de stockage d'origine, l'intégralité de votre installation Mirage, notamment la couche de base, la couche d'application, les données CVD, etc., est supprimée et devient irrécupérable si une sauvegarde n'est pas disponible.

Reportez-vous à « Installation d'Horizon FLEX Client pour des utilisateurs finaux », page 20 pour plus d'informations sur l'utilisation d'un déploiement en masse afin de fournir Horizon FLEX Client aux utilisateurs.

Journaux système d' Horizon FLEX

Les fichiers journaux d'Horizon FLEX peuvent être utilisés pour résoudre des problèmes du système.

Les journaux système d'Horizon FLEX sont disponibles aux emplacements suivants :

- Fichier journal d'application Web

  `C:\ProgramData\Wanova Mirage\rvm\logs\webapp.log`

- Journaux d'Horizon FLEX Server

  `C:\Program Files\Wanova\Mirage Management Server\logs`

  Le fichier journal le plus important est le fichier `mgmtservice.log`.

- Horizon FLEX utilise la fonction de jonction de domaine hors connexion de Microsoft. Le fichier journal de jonction de domaine hors connexion se trouve à l'emplacement suivant :

  `C:\Windows\debug\NetSetup.LOG`

Index