Administration de VMware Horizon View

Présentation 5.2

Présentation Manager 5.2

Présentation Composer 5.2

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-001024-00

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

Copyright © 2013 VMware, Inc. Tous droits réservés. Ce produit est protégé par les lois américaines et internationales relatives au copyright et à la propriété intellectuelle. Les produits VMware sont protégés par un ou plusieurs brevets répertoriés à l'adresse http://www.vmware.com/go/patents-fr.

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

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

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

Table des matières

Administration de VMware Horizon View

Le document *Administration de VMware Horizon View* décrit comment configurer et administrer VMware Horizon View™, y compris comment configurer Serveur de connexion View, créer des administrateurs, approvisionner et déployer des postes de travail View, configurer l'authentification utilisateur, configurer des règles et gérer des applications VMware ThinApp™ dans View Administrator. Ces informations décrivent également comment entretenir et dépanner des composants VMware Horizon View.

Public cible

Ces informations sont destinées à toute personne souhaitant configurer et administrer VMware Horizon View. Les informations sont destinées aux administrateurs système Windows ou Linux expérimentés qui connaissent bien le fonctionnement des datacenters et de la technologie des machines virtuelles.

Configuration de View Connection Server 1

Après avoir installé et effectué la configuration initiale de View Connection Server, vous pouvez ajouter des instances de vCenter Server et des services View Composer à View Manager, configurer des rôles pour déléguer des responsabilités d'administrateur et planifier des sauvegardes de vos données de configuration.

Ce chapitre aborde les rubriques suivantes :

Utilisation de View Administrator

View Administrator est l'interface Web dans laquelle vous configurez Serveur de connexion View et gérez vos postes de travail View.

Pour voir une comparaison des opérations que vous pouvez effectuer avec View Administrator, des cmdlets View et `vdmadmin`, consultez le document *Intégration de VMware Horizon View*.

View Administrator et View Connection Server

View Administrator fournit une interface de gestion pour View Manager.

En fonction de votre déploiement View, vous utilisez une ou plusieurs interfaces de View Administrator.

- Utilisez une interface de View Administrator pour gérer les composants View associés à une instance de View Connection Server autonome ou à un groupe d'instances de View Connection Server répliquées.

  Vous pouvez utiliser l'adresse IP de n'importe quelle instance répliquée pour ouvrir une session sur View Administrator.

- Vous devez utiliser une interface de View Administrator séparée pour gérer les composants View pour chaque instance de View Connection Server autonome ou chaque groupe d'instances de View Connection Server répliquées.

Vous pouvez également utiliser View Administrator pour gérer des serveurs de sécurité et des instances de View Transfer Server associés à View Connection Server.

- Chaque serveur de sécurité est associé à une instance de View Connection Server.
- Chaque instance de View Transfer Server peut communiquer avec n'importe quelle instance de View Connection Server dans un groupe d'instances répliquées.

Ouvrir une session sur View Administrator

Pour effectuer des tâches de configuration initiale, vous devez ouvrir une session sur View Administrator. Vous accédez à View Administrator via une connexion SSL.

Prérequis

- Vérifiez que Serveur de connexion View est installé sur un ordinateur dédié.
- Vérifiez que vous utilisez un navigateur Web pris en charge par View Administrator. Pour plus d'informations sur la configuration requise de View Administrator, consultez le document *Installation de VMware Horizon View*.

Procédure

1 Ouvrez votre navigateur Web et saisissez l'URL suivante, où *server* est le nom d'hôte de l'instance de Serveur de connexion View.

```
https://server/admin
```

Remarque Vous pouvez utiliser l'adresse IP si vous devez accéder à une instance de Serveur de connexion View lorsque le nom d'hôte n'est pas résolvable. Toutefois, l'hôte que vous contactez ne correspondra pas au certificat SSL configuré pour l'instance de Serveur de connexion View, ce qui se traduit par un accès bloqué ou un accès avec une sécurité réduite.

Votre accès à View Administrator dépend du type de certificat configuré sur l'ordinateur Serveur de connexion View.

Option	Description
Vous avez configuré un certificat signé par une autorité de certification pour Serveur de connexion View.	Lorsque vous vous connectez pour la première fois, votre navigateur Web affiche View Administrator.
Le certificat auto-signé par défaut fourni avec Serveur de connexion View est configuré.	À votre première connexion, votre navigateur Web peut afficher une page vous avertissant que le certificat de sécurité associé à l'adresse n'est pas émis par une autorité de certification approuvée. Cliquez sur **[Ignorer]** pour continuer à utiliser le certificat SSL actuel.

2 Ouvrez une session en tant qu'utilisateur actuel avec des informations d'identification pour accéder au compte View Administrators.

Vous spécifiez le compte View Administrators lorsque vous installez une instance autonome de Serveur de connexion View ou la première instance de Serveur de connexion View dans un groupe répliqué. Le compte View Administrators peut être le groupe Administrators local (BUILTIN\Administrators) sur l'ordinateur Serveur de connexion View ou un compte d'utilisateur ou de groupe de domaine.

Après avoir ouvert une session sur View Administrator, vous pouvez utiliser **[Configuration de View] > [Administrateurs]** pour modifier la liste d'utilisateurs et de groupes avec le rôle Administrateurs View.

Conseils d'utilisation de l'interface de View Administrator

Vous pouvez utiliser les fonctions d'interface utilisateur de View Administrator pour naviguer dans les pages de View et pour rechercher, filtrer et trier des objets View.

View Administrator comporte plusieurs fonctions d'interface utilisateur courantes. Par exemple, le volet de navigation à gauche de chaque page vous dirige vers d'autres pages de View Administrator. Les filtres de recherche vous permettent de sélectionner des critères de filtrage liés aux objets que vous recherchez.

Tableau 1-1 décrit des fonctions supplémentaires qui peuvent vous aider dans l'utilisation de View Administrator.

Tableau 1-1. Fonctions de navigation et d'affichage de View Administrator

Fonction de View Administrator	Description
Navigation vers l'arrière et vers l'avant dans les pages de View Administrator	Cliquez sur le bouton **[Back (Précédent)]** du navigateur pour retourner à la page précédente de View Administrator. Cliquez sur le bouton **[Forward (Suivant)]** pour revenir à la page actuelle. Si vous cliquez sur le bouton **[Back (Précédent)]** du navigateur lorsque vous utilisez l'assistant ou la boîte de dialogue View Administrator, vous revenez à la page principale de View Administrator. Les informations que vous avez entrées dans l'assistant ou la boîte de dialogue sont perdues. Dans les versions View antérieures à View 5.1, vous ne pouviez pas utiliser les boutons **[Back (Précédent)]** et **[Forward (Suivant)]** du navigateur pour naviguer dans View Administrator. Il existait des boutons **[Back (Précédent)]** et **[Forward (Suivant)]** distincts pour la navigation dans la fenêtre View Administrator. Ces boutons ne figurent plus dans la version View 5.1.
Affectation de signets aux pages View Administrator	Vous pouvez affecter des signets aux pages View Administrator dans le navigateur.
Tri multicolonne	Vous pouvez trier des objets View de plusieurs façons en utilisant le tri multicolonne. Cliquez sur un titre dans la ligne supérieure d'un tableau View Administrator pour trier les objets View par ordre alphabétique par rapport à ce titre. Par exemple, sur la page **[Inventory (Inventaire)] > [Postes de travail]** , vous pouvez cliquer sur **[Pool]** pour trier les postes de travail en fonction des pools qui les contiennent. Le nombre **[1]** apparaît à côté du titre pour indiquer qu'il s'agit de la principale colonne de tri. Vous pouvez cliquer de nouveau sur le titre pour inverser l'ordre de tri, indiqué par une flèche vers le bas ou vers le haut. Pour trier les objets View en fonction d'un deuxième élément, appuyez sur Ctrl +clic sur un autre titre. Par exemple, dans le tableau **[Desktops (Postes de travail)]** , vous pouvez cliquer sur **[Users (Utilisateurs)]** pour effectuer un deuxième tri en fonction des utilisateurs auxquels les postes de travail sont dédiés. Le nombre **[2]** apparaît à côté du titre secondaire. Dans cet exemple, les postes de travail sont triés par pool et par utilisateurs dans chaque pool. Vous pouvez continuer à utiliser Ctrl+clic pour trier toutes les colonnes d'un tableau par ordre décroissant d'importance. Appuyez sur Ctrl+Maj+clic pour désélectionner un élément de tri. Par exemple, vous souhaitez afficher les postes de travail dans un pool qui sont dans un état particulier et sont stockés dans un magasin de données particulier. Vous pouvez cliquer sur **[Inventory (Inventaire)] > [Pools]** , double-cliquer sur l'ID de pool, cliquer sur l'onglet Inventory (Inventaire) et sur l'en-tête **[Datastore (Magasin de données)]** et appuyer sur Ctrl et cliquer simultanément sur l'en-tête **[Status (État)]** .

Tableau 1-1. Fonctions de navigation et d'affichage de View Administrator (suite)

Fonction de View Administrator	Description
Personnalisation des colonnes des tables	Vous pouvez personnaliser l'affichage des colonnes des tables View Administrator en masquant des colonnes et en verrouillant la première colonne. Cette fonction permet de contrôler l'affichage des grandes tables, telles que **[Inventory (Inventaire)] > [Desktops (Postes de travail)]** qui contiennent de nombreuses colonnes. Cliquez avec le bouton droit de la souris sur un en-tête de colonne pour afficher un menu contextuel qui permet d'exécuter les actions suivantes : ■ Masquer la colonne sélectionnée. ■ Personnaliser les colonnes. Une boîte de dialogue affiche toutes les colonnes de la table. Vous pouvez sélectionner les colonnes à afficher ou masquer. ■ Verrouiller la première colonne. Cette option force l'affichage de la première colonne lorsque vous faites défiler horizontalement une table comportant un grand nombre de colonnes. Par exemple, dans la page **[Inventory (Inventaire)] > [Desktops (Postes de travail)]** , l'ID de poste de travail reste affiché lorsque vous faites défiler horizontalement les données pour afficher d'autres caractéristiques de poste de travail. Les paramètres personnalisés sont conservés lorsque vous restez dans la page View Administrator en cours. Ils ne sont plus disponibles si vous passez à une autre page.
Sélection d'objets View et affichage de détails sur l'objet View	Dans les tableaux View Administrator qui répertorient des objets View, vous pouvez sélectionner un objet ou afficher des détails sur l'objet. ■ Pour sélectionner un objet, cliquez n'importe où dans la ligne de l'objet dans le tableau. En haut de la page, les menus et les commandes qui gèrent l'objet deviennent actifs. ■ Pour afficher des détails sur l'objet, double-cliquez sur la cellule de gauche de la ligne de l'objet. Une nouvelle page affiche les détails de l'objet. Par exemple, sur la page **[Inventory (Inventaire)] > [Pools]** , cliquez n'importe où dans la ligne d'un pool individuel pour activer des commandes qui affectent le pool. Double-cliquez dans la cellule **[Pool ID (ID de pool)]** dans la colonne de gauche pour afficher une nouvelle page contenant des détails sur le pool.
Développer les boîtes de dialogue pour afficher les détails	Vous pouvez développer les boîtes de dialogue de View Administrator pour afficher dans les colonnes d'un tableau des détails tels que le nom des postes de travail et des utilisateurs. Pour développer une boîte de dialogue, placez le pointeur de votre souris au-dessus des points, dans le coin supérieur droit de la boîte de dialogue, puis faites glisser ce coin.
Affichage des menus contextuels des objets View.	Cliquez avec le bouton droit de la souris sur les objets View dans les tables View Administrator pour afficher des menus contextuels. Un menu contextuel permet d'accéder aux commandes qui agissent sur l'objet View sélectionné. Par exemple, dans la page **[Inventory (Inventaire)] > [Pools]** , vous pouvez cliquer avec le bouton droit de la souris sur un pool de postes de travail pour afficher des commandes, telles que **[Add (Ajouter)]** , **[Edit (Modifier)]** , **[Delete (Supprimer)]** , **[Disable (or Enable) Provisioning (Désactiver (ou Activer) le provisionnement)]** , etc.

Résolution des problèmes de l'affichage du texte dans View Administrator

Si votre navigateur Web s'exécute sur un système d'exploitation non Windows tel que Linux, UNIX ou Mac OS, le texte dans View Administrator ne s'affiche pas correctement.

Problème

Le texte dans l'interface de View Administrator est corrompu. Par exemple, des espaces sont placés au milieu des mots.

Cause

View Administrator requiert des polices spécifiques de Microsoft.

Solution

Installez des polices spécifiques de Microsoft sur votre ordinateur.

Actuellement, le site Web Microsoft ne distribue pas de polices Microsoft, mais vous pouvez les télécharger sur des sites Web indépendants.

Configuration de vCenter Server et View Composer

Pour utiliser des machines virtuelles en tant que sources de postes de travail, vous devez configurer View Manager pour communiquer avec vCenter Server. Pour créer et gérer des postes de travail de clone lié, vous devez configurer des paramètres de View Composer dans View Manager.

Vous pouvez également configurer des paramètres de stockage pour View. Vous pouvez autoriser les hôtes ESXi à récupérer de l'espace disque sur les machines virtuelles de clone lié. Pour permettre à des hôtes ESXi de mettre en cache des données de machine virtuelle, vous devez activer View Storage Accelerator pour vCenter Server.

Créer un compte d'utilisateur pour View Composer

Si vous utilisez View Composer, vous devez créer un compte d'utilisateur dans Active Directory pour l'utiliser avec View Composer. View Composer a besoin de ce compte pour associer des postes de travail de clone lié à votre domaine Active Directory.

Pour garantir la sécurité, vous devez créer un compte d'utilisateur séparé à utiliser avec View Composer. En créant un compte séparé, vous pouvez garantir qu'il n'a pas de privilèges supplémentaires définis pour une autre raison. Vous pouvez donner au compte les privilèges minimum dont il a besoin pour créer et supprimer des objets ordinateur dans un conteneur Active Directory spécifié. Par exemple, le compte View Composer ne requiert pas de privilèges d'administrateur de domaine.

Procédure

1 Dans Active Directory, créez un compte d'utilisateur dans le même domaine que votre hôte de Serveur de connexion View ou dans un domaine approuvé.

2 Ajoutez les autorisations **[Créer des objets ordinateur]** , **[Supprimer des objets ordinateur]** et **[Écrire toutes les propriétés]** au compte dans le conteneur Active Directory dans lequel les comptes d'ordinateur de clone lié sont créés ou vers lequel les comptes d'ordinateur de clone lié sont déplacés.

   La liste suivante montre toutes les autorisations requises pour le compte d'utilisateur, y compris les autorisations affectées par défaut :

   - Contenu de la liste
   - Lire toutes les propriétés
   - Écrire toutes les propriétés
   - Lire les autorisations
   - Réinitialiser le mot de passe
   - Créer des objets ordinateur

- Supprimer des objets ordinateur

Remarque Si vous sélectionnez le paramètre **[Autoriser la réutilisation de comptes d'ordinateur pré-existants]** pour un pool de postes de travail, vous avez seulement besoin d'ajouter les autorisations suivantes :

- Contenu de la liste
- Lire toutes les propriétés
- Lire les autorisations
- Réinitialiser le mot de passe

3 Assurez-vous que les autorisations du compte d'utilisateur s'appliquent au conteneur Active Directory et à tous les objets enfants du conteneur.

Suivant

Spécifiez le compte dans View Administrator lorsque vous configurez View Composer pour vCenter Server et quand vous configurez et déployez des pools de postes de travail de clone lié.

Ajouter des instances de vCenter Server à View Manager

Vous devez configurer View Manager pour vous connecter aux instances de vCenter Server dans votre déploiement de View. vCenter Server crée et gère les machines virtuelles que View Manager utilise en tant que sources de postes de travail.

Si vous exécutez des instances de vCenter Server sur un groupe Mode lié, vous devez ajouter chaque instance de vCenter Server sur View Manager séparément.

View Manager se connecte à l'instance de vCenter Server via un canal sécurisé (SSL).

Prérequis

- Installez la clé de licence produit de Serveur de connexion View.
- Préparez un utilisateur de vCenter Server avec une autorisation d'effectuer les opérations dans vCenter Server qui sont nécessaires pour prendre en charge View Manager. Pour utiliser View Composer, vous devez accorder à l'utilisateur des privilèges supplémentaires. Pour gérer des postes de travail utilisés en mode local, vous devez accorder à l'utilisateur des privilèges en plus de ceux requis pour View Manager et View Composer.

  Pour plus d'informations sur la configuration d'un utilisateur de vCenter Server pour View Manager, consultez le document *Installation de VMware Horizon View*.
- Vérifiez qu'un certificat de serveur SSL est installé sur l'hôte de vCenter Server. Dans un environnement de production, installez un certificat SSL valide signé par une autorité de certification approuvée.

  Dans un environnement de test, vous pouvez utiliser le certificat par défaut qui est installé avec vCenter Server, mais vous devez accepter l'empreinte numérique de certificat lorsque vous ajoutez vCenter Server à View.
- Vérifiez que toutes les instances de Serveur de connexion View dans le groupe répliqué approuvent le certificat de l'autorité de certification racine pour le certificat de serveur qui est installé sur l'hôte de vCenter Server. Vérifiez si le certificat de l'autorité de certification racine se trouve dans le dossier **[Autorités de certification racine de confiance] > [Certificats]** dans les magasins de certificats de l'ordinateur local Windows sur les hôtes de Serveur de connexion View. Si ce n'est pas le cas, importez le certificat de l'autorité de certification racine dans les magasins de certificats de l'ordinateur local Windows.

  Consultez la section « Importer un certificat racine et des certificats intermédiaires dans un magasin de certificats Windows » dans le document *Installation de VMware Horizon View*.

- Vérifiez que l'instance de vCenter Server contient des hôtes ESXi. Si aucun hôte n'est configuré dans l'instance de vCenter Server, vous ne pouvez pas ajouter l'instance à View.
- Familiarisez-vous avec les paramètres qui déterminent les limites d'opérations maximales pour vCenter Server et View Composer. Reportez-vous aux sections « Nombre maximal d'opérations simultanées pour vCenter Server et View Composer », page 23 et « Définition d'un taux d'opérations d'alimentation simultanées pour prendre en charge les tempêtes d'ouverture de session des postes de travail View », page 24.

Procédure

1 Dans View Administrator, cliquez sur **[Configuration de View] > [Serveurs]** .

2 Sous l'onglet vCenter Servers, cliquez sur **[Ajouter]** .

3 Dans la zone de texte de l'adresse du serveur vCenter Server Settings (Paramètres de vCenter Server), saisissez le nom de domaine complet (FQDN) de l'instance de vCenter Server.

Le FQDN inclut le nom d'hôte et le nom de domaine. Par exemple, dans le FQDN ***myserverhost.companydomain.com***, ***myserverhost*** est le nom d'hôte et ***companydomain.com*** le domaine.

REMARQUE Si vous saisissez un serveur à l'aide d'un nom DNS ou d'une URL, View Manager n'effectue pas de recherche DNS pour vérifier si un administrateur a précédemment ajouté ce serveur à View Manager à l'aide de son adresse IP. Un conflit se produit si vous ajoutez un serveur vCenter Server avec son nom DNS et son adresse IP.

4 Saisissez le nom de l'utilisateur de vCenter Server.

Par exemple : **domain\user** ou **user@domain.com**

5 Saisissez le mot de passe de l'utilisateur de vCenter Server.

6 (Facultatif) Saisissez une description de cette instance de vCenter Server.

7 Saisissez le numéro du port TCP.

Le port par défaut est 443.

8 Sous Paramètres avancés, définissez les limites d'opérations simultanées pour les opérations de vCenter Server et View Composer.

9 Cliquez sur **[Suivant]** pour afficher la page Paramètres de View Composer.

Suivant

Configurez les paramètres de View Composer.

- Si l'instance de vCenter Server est configurée avec un certificat SSL signé et si Serveur de connexion View approuve le certificat racine, l'assistant Ajouter un serveur vCenter Server affiche la page Paramètres de View Composer.
- Si l'instance de vCenter Server est configurée avec un certificat par défaut, vous devez d'abord déterminer si vous acceptez l'empreinte numérique du certificat existant. Reportez-vous à la section « Accepter l'empreinte numérique d'un certificat SSL par défaut », page 24.

Si View Manager utilise plusieurs instances de vCenter Server, répétez cette procédure pour ajouter les autres instances de vCenter Server.

Configurer les paramètres de View Composer

Pour utiliser View Composer, vous devez configurer des paramètres qui permettent à View Manager de se connecter au service View Composer. View Composer peut être installé sur son propre hôte séparé ou sur le même hôte que vCenter Server.

Il doit exister un mappage un-à-un entre chaque service View Composer et instance de vCenter Server. Un service View Composer peut fonctionner avec une seule instance de vCenter Server. Une instance de vCenter Server peut être associée à un seul service View Composer.

Après le déploiement initial de View, vous pouvez migrer le service View Composer vers un nouvel hôte pour prendre en charge un déploiement de View croissant ou changeant. Vous pouvez modifier les paramètres initiaux de View Composer dans View Administrator, mais vous devez effectuer des étapes supplémentaires pour vous assurer que la migration réussit. Reportez-vous à la section « Migrer View Composer vers un autre ordinateur », page 416.

Prérequis

- Vérifiez que vous avez créé un utilisateur dans Active Directory avec l'autorisation d'ajouter et de supprimer des machines virtuelles du domaine Active Directory contenant vos clones liés. Reportez-vous à la section « Créer un compte d'utilisateur pour View Composer », page 15.
- Vérifiez que vous avez configuré View Manager pour vous connecter à vCenter Server. Pour cela, vous devez compléter la page Informations sur vCenter Server de l'assistant Ajouter un serveur vCenter Server. Reportez-vous à la section « Ajouter des instances de vCenter Server à View Manager », page 16.
- Vérifiez que ce service View Composer n'est pas déjà configuré pour se connecter à une instance de vCenter Server différente.

Procédure

1 Dans View Administrator, complétez la page Informations sur vCenter Server de l'assistant Ajouter un serveur vCenter Server.

   a Cliquez sur **[Configuration de View] > [Serveurs]** .

   b Sous l'onglet vCenter Server, cliquez sur **[Ajouter]** et fournissez les paramètres de vCenter Server.

2 Sur la page Paramètres de View Composer, si vous n'utilisez pas View Composer, sélectionnez **[Ne pas utiliser View Composer]** .

   Si vous sélectionnez **[Ne pas utiliser View Composer]** , les autres paramètres de View Composer deviennent inactifs. Lorsque vous cliquez sur **[Suivant]** , l'assistant Ajouter un serveur vCenter Server affiche la page Paramètres de stockage. La page Domaines View Composer ne s'affiche pas.

3 Si vous utilisez View Composer, sélectionnez l'emplacement de l'hôte de View Composer.

Option	Description
View Composer est installé sur le même hôte que vCenter Server.	a Sélectionnez **[View Composer est co-installé avec vCenter Server]** . b Vérifiez que le numéro de port est le même que le port spécifié lors de l'installation du service View Composer sur vCenter Server. Le numéro de port par défaut est 18443.
View Composer est installé sur son propre hôte séparé.	a Sélectionnez **[Serveur View Composer Server autonome]** . b Dans la zone de texte de l'adresse du serveur View Composer, saisissez le nom de domaine complet (FQDN) de l'hôte de View Composer. c Saisissez le nom de l'utilisateur de View Composer. Par exemple : **`domain.com\user`** ou **`user@domain.com`** d Saisissez le mot de passe de l'utilisateur de View Composer. e Vérifiez que le numéro de port est le même que le port spécifié lors de l'installation du service View Composer. Le numéro de port par défaut est 18443.

4 Cliquez sur **[Suivant]** pour afficher la page Domaines View Composer.

Suivant

Configurez les domaines de View Composer.

- Si l'instance de View Composer est configurée avec un certificat SSL signé et si Serveur de connexion View approuve le certificat racine, l'assistant Ajouter un serveur vCenter Server affiche la page Domaines View Composer.
- Si l'instance de View Composer est configurée avec un certificat par défaut, vous devez d'abord déterminer si vous acceptez l'empreinte numérique du certificat existant. Reportez-vous à la section « Accepter l'empreinte numérique d'un certificat SSL par défaut », page 24.

Configurer les domaines de View Composer

Vous devez configurer un domaine Active Directory dans lequel View Composer déploie des postes de travail de clone lié. Vous pouvez configurer plusieurs domaines pour View Composer. Après avoir ajouté des paramètres de vCenter Server et View Composer à View, vous pouvez ajouter plus de domaines View Composer en modifiant l'instance de vCenter Server dans View Administrator.

Prérequis

Dans View Administrator, vérifiez que vous avez rempli les pages vCenter Server Information (Informations sur vCenter Server) et View Composer Settings (Paramètres de View Composer) dans l'assistant Add vCenter Server (Ajouter un serveur vCenter Server).

Procédure

1 Sur la page View Composer Domains (Domaines View Composer), cliquez sur **[Ajouter]** pour ajouter l'utilisateur de domaine aux informations du compte View Composer.

2 Saisissez le nom de domaine du domaine Active Directory.

Par exemple : **`domain.com`**

3 Saisissez le nom de l'utilisateur de domaine, y compris le nom de domaine.

Par exemple : **`domain.com\admin`**

4 Saisissez le mot de passe du compte.

5 Cliquez sur **[OK]** .

6 Pour ajouter des comptes d'utilisateur de domaine avec des privilèges dans d'autres domaines Active Directory dans lesquels vous déployez des pools de clone lié, répétez les étapes précédentes.

7 Cliquez sur **[Suivant]** pour afficher la page Paramètres de stockage.

Suivant

Activez la récupération d'espace disque de machine virtuelle et configurez View Storage Accelerator pour View.

Autoriser vSphere à récupérer de l'espace disque dans des machines virtuelles de clone lié

Dans vSphere 5.1 et supérieur, vous pouvez activer la fonction de récupération d'espace disque pour View. À partir de vSphere 5.1, View crée des machines virtuelles de clone lié dans un format de disque efficace qui permet à des hôtes ESXi de récupérer l'espace disque inutilisé dans les clones liés, ce qui réduit l'espace de stockage total requis pour les clones liés.

Comme les utilisateurs interagissent avec des postes de travail de clone lié, les disques du système d'exploitation des clones croissent et peuvent finir par utiliser presque autant d'espace disque que les postes de travail de clone complet. La récupération d'espace disque réduit la taille des disques du système d'exploitation sans que vous ayez à actualiser ou recomposer les clones liés. L'espace peut être récupéré lorsque les machines virtuelles sont activées et que les utilisateurs interagissent avec leurs postes de travail.

La récupération d'espace disque est particulièrement utile pour les déploiements qui ne peuvent pas bénéficier de stratégies d'économie de stockage, telles que l'actualisation à la fermeture de session. Par exemple, les travailleurs du savoir qui installent des applications utilisateur sur des postes de travail dédiés peuvent perdre leurs applications personnelles si les postes de travail ont été actualisés ou recomposés. Avec la récupération d'espace disque, View peut conserver les clones liés proches de la taille réduite avec laquelle ils démarrent lors de leur premier approvisionnement.

Cette fonction comporte deux composants : format de disque à optimisation d'espace et opérations de récupération d'espace.

Dans un environnement vSphere 5.1 ou supérieur, lorsqu'une machine virtuelle parente est la version matérielle virtuelle 9 ou supérieure, View crée des clones liés avec des disques du système d'exploitation à optimisation d'espace, que les opérations de récupération d'espace soient activées ou non.

Pour activer les opérations de récupération d'espace, vous devez utiliser View Administrator afin d'activer la récupération d'espace pour vCenter Server et récupérer l'espace de disque de machine virtuelle pour des pools de postes de travail individuels. Le paramètre de récupération d'espace de vCenter Server vous permet de désactiver cette fonction sur tous les pools de postes de travail qui sont gérés par l'instance de vCenter Server. La désactivation de la fonction pour vCenter Server remplace le paramètre au niveau du pool de postes de travail.

Les recommandations suivantes s'appliquent à la fonction de récupération d'espace :

- Elle fonctionne uniquement sur les disques du système d'exploitation à optimisation d'espace dans des clones liés.
- Il n'affecte pas les disques persistants de View Composer.
- Elle fonctionne uniquement avec vSphere 5.1 ou supérieur et uniquement sur des postes de travail avec la version matérielle virtuelle 9 ou supérieure.
- Elle ne fonctionne pas sur les postes de travail de clone complet.
- Elle fonctionne sur les machines virtuelles avec des contrôleurs SCSI. Les contrôleurs IDE ne sont pas pris en charge.
- Elle fonctionne uniquement sur les postes de travail Windows XP et Windows 7. Elle ne fonctionne pas sur les postes de travail Windows 8.

La technologie de snapshot NFS natif (VAAI) n'est pas prise en charge dans les pools contenant des machines virtuelles avec des disques à optimisation d'espace.

Prérequis

- Vérifiez que vos hôtes de vCenter Server et ESXi sont à la version 5.1 avec le correctif de téléchargement ESXi 5.1 ESXi510-201212001 ou supérieur.

  Dans un cluster ESXi, vérifiez que tous les hôtes sont à la version 5.1 avec le correctif de téléchargement ESXi510-201212001 ou supérieur.

Procédure

1 Dans View Administrator, complétez les pages de l'assistant Ajouter un serveur vCenter Server qui précèdent la page Paramètres de stockage.

   a Sélectionnez **[Configuration de View] > [Serveurs]** .

   b Sous l'onglet Serveurs vCenter Server, cliquez sur **[Ajouter]** .

   c Complétez les pages Informations sur vCenter Server, Paramètres de View Composer et Domaines View Composer.

2 Sur la page Paramètres de stockage, vérifiez que **[Activer la récupération d'espace]** est sélectionné.

   La récupération d'espace est sélectionnée par défaut si vous effectuez une nouvelle installation de View 5.2 ou supérieur. Vous devez sélectionner **[Activer la récupération d'espace]** si vous effectuez une mise à niveau vers View 5.2 ou supérieur depuis View 5.1 ou une version antérieure.

Suivant

Sur la page Paramètres de stockage, configurez View Storage Accelerator.

Pour terminer la configuration de la récupération d'espace disque dans View, configurez la récupération d'espace pour les pools de postes de travail.

Configurer View Storage Accelerator pour vCenter Server

Dans vSphere 5.0 et supérieur, vous pouvez configurer des hôtes ESXi pour mettre en cache des données de disque de machine virtuelle. Cette fonction, appelée View Storage Accelerator, utilise la fonction CBRC (Content Based Read Cache) dans les hôtes ESXi. View Storage Accelerator améliore les performances de View lors des tempêtes d'E/S, qui peuvent se produire lorsque de nombreux postes de travail démarrent ou exécutent des analyses antivirus simultanément. La fonction est également utile lorsque des administrateurs ou des utilisateurs chargent des applications ou des données fréquemment. Au lieu de lire tout le système d'exploitation ou l'application depuis le système de stockage encore et encore, un hôte peut lire des blocs de données communes depuis le cache.

En réduisant le nombre d'IOPS au cours des tempêtes de démarrage, View Storage Accelerator diminue la demande sur la baie de stockage. Vous pouvez ainsi utiliser moins de bande passante d'E/S de stockage pour prendre en charge votre déploiement de View.

Vous activez la mise en cache sur vos hôtes ESXi en sélectionnant le paramètre View Storage Accelerator dans l'assistant vCenter Server dans View Administrator, comme décrit dans cette procédure.

Vérifiez que View Storage Accelerator est également configuré pour des pools de postes de travail individuels. View Storage Accelerator est activé pour les pools par défaut, mais cette fonction peut être désactivée ou activée lorsque vous créez ou modifiez un pool. Pour fonctionner sur un pool, View Storage Accelerator doit être activé pour vCenter Server et pour le pool individuel.

Vous pouvez activer View Storage Accelerator sur des pools contenant des clones liés et sur des pools contenant des machines virtuelles complètes.

View Storage Accelerator est également pris en charge avec le mode local. Les utilisateurs peuvent emprunter des postes de travail dans des pools activés pour View Storage Accelerator. View Storage Accelerator est désactivé lorsqu'un poste de travail est emprunté et réactivé lorsque le poste de travail est restitué.

La technologie de snapshot NFS natif (VAAI) n'est pas prise en charge dans les pools activés pour View Storage Accelerator.

View Storage Accelerator est maintenant conçu pour fonctionner dans des configurations qui utilisent la hiérarchisation de réplica View, dans lesquelles des réplicas sont stockés dans un magasin de données séparé des clones liés. Bien que les avantages de performance de l'utilisation de View Storage Accelerator avec la hiérarchisation de réplica View ne soient pas matériellement importants, certains avantages liés à la capacité peuvent être atteints en stockant les réplicas sur un magasin de données séparé. Par conséquent, cette combinaison est testée et prise en charge.

Prérequis

- Vérifiez que vos hôtes vCenter Server et ESXi sont les versions 5.0 ou supérieures.

  Dans un cluster ESXi, vérifiez que la version de tous les hôtes est la version 5.0 ou supérieure.

- Vérifiez que l'utilisateur de vCenter Server s'est vu affecté le privilège **Général > Agir comme vCenter Server** dans vCenter Server. Consultez les rubriques dans la documentation *Installation de VMware Horizon View* qui décrivent les privilèges de View Manager et de View Composer requis pour l'utilisateur de vCenter Server.

Procédure

1 Dans View Administrator, complétez les pages de l'assistant Ajouter un serveur vCenter Server qui précèdent la page Paramètres de stockage.

   a Sélectionnez **[Configuration de View]** > **[Serveurs]** .

   b Sous l'onglet Serveurs vCenter Server, cliquez sur **[Ajouter]** .

   c Complétez les pages Informations sur vCenter Server, Paramètres de View Composer et Domaines View Composer

2 Sur la page Paramètres de stockage, vérifiez que la case **[Activer View Storage Accelerator]** est cochée.

   Cette case est cochée par défaut.

3 Spécifiez une taille par défaut pour le cache de l'hôte.

   La taille de cache par défaut s'applique à tous les hôtes ESXi gérés par cette instance de vCenter Server.

   La valeur par défaut est 1 024 Mo. La taille de cache doit être comprise entre 100 Mo et 2 048 Mo.

4 Pour spécifier une taille de cache différente pour un hôte ESXi en particulier, sélectionnez un hôte ESXi et cliquez sur **[Modifier la taille de cache]** .

   a Dans la boîte de dialogue Cache de l'hôte, cochez la case **[Remplacer la taille de cache de l'hôte par défaut]** .

   b Saisissez une valeur **[Taille de cache de l'hôte]** comprise entre 100 Mo et 2 048 Mo et cliquez sur **[OK]** .

5 Sur la page Paramètres de stockage, cliquez sur **[Suivant]** .

6 Cliquez sur **[Terminer]** pour ajouter vCenter Server, View Composer et Paramètres de stockage à View.

Suivant

Configurez des paramètres pour les sessions et les connexions client. Reportez-vous à la section « Configuration de paramètres pour des sessions client », page 27.

Pour régler les paramètres de View Storage Accelerator dans View, configurez View Storage Accelerator pour des pools de postes de travail. Reportez-vous à la section « Configurer View Storage Accelerator pour des pools de postes de travail », page 167.

Nombre maximal d'opérations simultanées pour vCenter Server et View Composer

Lorsque vous ajoutez vCenter Server à View ou modifiez les paramètres vCenter Server, vous pouvez configurer plusieurs options qui définissent le nombre maximal d'opérations simultanées exécutées par vCenter Server et View Composer.

Vous définissez ces options dans le panneau des paramètres avancés de la page des informations vCenter Server.

Tableau 1-2. Nombre maximal d'opérations simultanées pour vCenter Server et View Composer

Paramètre	Description
[Max concurrent vCenter provisioning operations (Opérations d'approvisionnement de vCenter simultanées max.)]	Ce paramètre détermine le nombre maximal de demandes simultanées que View Manager peut créer pour approvisionner et supprimer des machines virtuelles complètes dans cette instance de vCenter Server. La valeur par défaut est 20. Le paramètre s'applique uniquement aux machines virtuelles complètes.
[Opérations d'alimentation simultanées max.]	Ce paramètre détermine le nombre maximal d'opérations d'alimentation (démarrage, arrêt, interruption, etc.) pouvant se dérouler simultanément sur les machines virtuelles gérées par View Manager dans l'instance de vCenter Server. La valeur par défaut est 50. Pour les instructions de calcul d'une valeur pour ce paramètre, voir « Définition d'un taux d'opérations d'alimentation simultanées pour prendre en charge les tempêtes d'ouverture de session des postes de travail View », page 24. Le paramètre s'applique uniquement aux machines virtuelles complètes et aux clones liés.
[Max concurrent View Composer maintenance operations (Nombre max. d'opérations de maintenance View Composer simultanées)]	Détermine le nombre maximal d'opérations d'actualisation, de recomposition et de rééquilibrage View Composer pouvant se dérouler simultanément sur les clones liés gérés par l'instance de View Composer. La valeur par défaut est 12. Si des sessions sont actives sur des postes de travail, elles doivent être fermées pour qu'une opération de maintenance puisse commencer. Si vous forcez les utilisateurs à fermer les sessions dès qu'une opération de maintenance commence, le nombre maximal d'opérations simultanées sur les postes de travail dont les sessions doivent être fermées est égal à la moitié de la valeur définie. Par exemple, si vous affectez à ce paramètre la valeur 24 et que vous forciez les utilisateurs à fermer leur session, le nombre maximal d'opérations simultanées sur les postes de travail dont les sessions doivent être fermées est égal à 12. Le paramètre ne s'applique qu'aux clones liés.
[Max concurrent View Composer provisioning operations (Nombre max. d'opérations d'approvisionnement View Composer simultanées)]	Détermine le nombre maximal d'opérations de création et de suppression pouvant se dérouler simultanément sur les clones liés gérés par l'instance de View Composer. La valeur par défaut est 8. Le paramètre ne s'applique qu'aux clones liés.

Définition d'un taux d'opérations d'alimentation simultanées pour prendre en charge les tempêtes d'ouverture de session des postes de travail View

Le paramètre **[Opérations d'alimentation simultanées max]** régit le nombre maximal d'opérations d'alimentation simultanées qui se produisent sur des machines virtuelles de poste de travail View dans une instance de vCenter Server. À partir de View 5.0, cette limite est définie sur 50 par défaut. Vous pouvez modifier cette valeur pour prendre en charge les taux maximaux d'activation lorsque de nombreux utilisateurs se connectent à leurs postes de travail en même temps.

Il est recommandé de réaliser une phase pilote afin de déterminer la valeur correcte de ce paramètre. Pour voir des recommandations sur la planification, consultez la section « Recommandations sur la planification et les éléments de conception d'architecture » dans le document *Planification de l'architecture de VMware Horizon View*.

Le nombre requis d'opérations d'alimentation simultanées se base sur le taux maximal auquel les postes de travail sont activés et sur la durée nécessaire au poste de travail pour s'activer, démarrer et devenir disponible pour la connexion. En général, la limite d'opérations d'alimentation recommandée est la durée totale nécessaire au poste de travail pour démarrer multipliée par le taux d'activation maximal.

Par exemple, un poste de travail moyen prend entre deux et trois minutes pour démarrer. Par conséquent, la limite d'opérations d'alimentation simultanées doit être 3 fois le taux d'activation maximal. Le paramètre par défaut de 50 devrait prendre en charge un taux d'activation maximal de 16 postes de travail par minute.

View attend cinq minutes au maximum qu'un poste de travail démarre. Si la durée de démarrage est plus longue, d'autres erreurs peuvent se produire. Pour être classique, vous pouvez définir une limite d'opérations d'alimentation simultanées de 5 fois le taux d'activation maximal. Avec une approche classique, le paramètre par défaut de 50 prend en charge un taux d'activation maximal de 10 postes de travail par minute.

Les ouvertures de session, et donc les opérations d'activation de poste de travail, se produisent en général d'une façon normalement distribuée sur une certaine fenêtre de temps. Vous pouvez estimer le taux d'activation maximal en supposant qu'il se produise au milieu de la fenêtre de temps, quand environ 40 % des opérations d'activation se produisent dans 1/6ème de la fenêtre de temps. Par exemple, si des utilisateurs ouvrent une session entre 8h00 et 9h00, la fenêtre de temps est d'une heure et 40 % des ouvertures de session se produisent dans les 10 minutes entre 8h25 et 8h35. S'il y a 2 000 utilisateurs, dont 20 % ont leurs postes de travail désactivés, alors 40 % des 400 opérations d'activation de poste de travail se produisent dans ces 10 minutes. Le taux d'activation maximal est de 16 postes de travail par minute.

Accepter l'empreinte numérique d'un certificat SSL par défaut

Lorsque vous ajoutez des instances de vCenter Server et View Composer à Horizon View, vous devez vérifier que les certificats SSL qui sont utilisés pour les instances de vCenter Server et View Composer sont valides et approuvées par Serveur de connexion View. Si les certificats par défaut qui sont installés avec vCenter Server et View Composer sont toujours en place, vous devez choisir d'accepter ou non les empreintes numériques de ces certificats.

Si une instance de vCenter Server ou View Composer est configurée avec un certificat signé par une autorité de certification, et si le certificat racine est approuvé par Serveur de connexion View, vous n'avez pas à accepter l'empreinte numérique de certificat. Aucune action n'est requise.

Si vous remplacez un certificat par défaut par un certificat signé par une autorité de certification, mais que Serveur de connexion View n'approuve pas le certificat racine, vous devez déterminer si vous acceptez l'empreinte numérique de certificat. Une empreinte numérique est un hachage cryptographique d'un certificat. L'empreinte numérique est utilisée pour déterminer rapidement si un certificat présenté est le même qu'un autre certificat, tel que le certificat qui a été accepté précédemment.

Remarque Si vous installez vCenter Server et View Composer sur le même hôte Windows Server, ils peuvent utiliser le même certificat SSL, mais vous devez configurer le certificat séparément pour chaque composant.

Pour plus d'informations sur la configuration des certificats SSL, consultez la section « Configuration de certificats SSL pour des serveurs View Server » dans le document *Installation de VMware Horizon View*.

Vous ajoutez d'abord vCenter Server et View Composer dans View Administrator à l'aide de l'assistant Ajouter un serveur vCenter Server. Si un certificat n'est pas approuvé et si vous n'acceptez pas l'empreinte numérique, vous ne pouvez pas ajouter vCenter Server et View Composer.

Une fois que ces serveurs sont ajoutés, vous pouvez les reconfigurer dans la boîte de dialogue Modifier vCenter Server.

Remarque Vous devez également accepter une empreinte numérique de certificat lorsque vous effectuez une mise à niveau depuis une version antérieure à Horizon View 5.1 ou supérieur, et lorsqu'un certificat de vCenter Server ou View Composer n'est pas approuvé, ou si vous remplacez un certificat approuvé par un certificat non approuvé.

Sur le tableau de bord de View Administrator, l'icône de vCenter Server ou View Composer devient rouge et la boîte de dialogue Certificat non valide détecté s'affiche. Vous devez cliquer sur **[Vérifier]** et suivre la procédure indiquée ici.

De la même façon, dans View Administrator, vous pouvez configurer un authentificateur SAML 2.0 qu'utilisera une instance de Serveur de connexion View. Si le certificat de serveur SAML 2.0 n'est pas approuvé par Serveur de connexion View, vous devez déterminer si vous acceptez l'empreinte numérique de certificat. Si vous n'acceptez pas l'empreinte numérique, vous ne pouvez pas configurer l'authentificateur SAML 2.0 dans Horizon View. Une fois que l'authentificateur SAML 2.0 est configuré, vous pouvez le reconfigurer dans la boîte de dialogue Modifier Serveur de connexion View.

Procédure

1 Lorsque View Administrator affiche la boîte de dialogue Certificat non valide détecté, cliquez sur **[Afficher le certificat]** .

2 Examinez l'empreinte numérique de certificat dans la fenêtre Informations sur le certificat.

3 Examinez l'empreinte numérique de certificat qui a été configurée pour l'instance de vCenter Server ou View Composer.

   a Sur l'hôte de vCenter Server ou View Composer, démarrez le composant logiciel MMC et ouvrez le magasin de certificats Windows.

   b Allez au certificat de vCenter Server ou View Composer.

   c Cliquez sur l'onglet Détails du certificat pour afficher l'empreinte numérique de certificat.

   De la même façon, examinez l'empreinte numérique de certificat pour un authentificateur SAML 2.0. Le cas échéant, réalisez les étapes précédentes sur l'hôte d'authentificateur SAML 2.0.

4 Vérifiez que l'empreinte numérique dans la fenêtre Informations sur le certificat correspond à l'empreinte numérique de l'instance de vCenter Server ou View Composer.

   De la même façon, vérifiez que les empreintes numériques correspondent pour un authentificateur SAML 2.0.

5 Déterminez si vous acceptez l'empreinte numérique de certificat.

Option	Description
Les empreintes numériques correspondent.	Cliquez sur **[Accepter]** pour utiliser le certificat par défaut.
Les empreintes numériques ne correspondent pas.	Cliquez sur **[Refuser]** . Corrigez les certificats incompatibles. Par exemple, vous avez peut-être fourni une adresse IP incorrecte pour vCenter Server ou View Composer.

Supprimer une instance de vCenter Server de View Manager

Vous pouvez supprimer la connexion entre View Manager et une instance de vCenter Server. Lorsque vous faites cela, View Manager ne gère plus les postes de travail View créés dans cette instance de vCenter Server.

Prérequis

Supprimez tous les postes de travail View associés à l'instance de vCenter Server. Reportez-vous à la section « Supprimer un pool de postes de travail de View Manager », page 310.

Procédure

1 Cliquez sur **[View Configuration (Configuration de View)] > [Servers (Serveurs)]** .

2 Dans le volet vCenter Servers (Serveurs vCenter Server), sélectionnez l'instance de vCenter Server.

3 Cliquez sur **[Remove (Supprimer)]** .

Une boîte de dialogue vous avertit que View Manager n'a plus accès aux machines virtuelles gérées par cette instance de vCenter Server.

4 Cliquez sur **[OK]** .

View Manager ne peut plus accéder aux machines virtuelles créées dans l'instance de vCenter Server.

Supprimer View Composer de View Manager

Vous pouvez supprimer la connexion entre View Manager et le service View Composer associé à une instance de vCenter Server.

Avant de désactiver la connexion à View Composer, vous devez supprimer tous les postes de travail de clone lié créés par View Composer de View Manager. View Manager vous empêche de supprimer View Composer si des clones liés associés existent toujours. Une fois la connexion à View Composer désactivée, View Manager ne peut pas provisionner ou gérer les nouveaux clones liés.

Procédure

1 Supprimez les pools de clone lié créés par View Composer.

a Dans View Administrator, cliquez sur **[Inventory (Inventaire)] > [Pools]** .

b Sélectionnez un pool de clone lié et cliquez sur **[Delete (Supprimer)]** .

Une boîte de dialogue vous avertit que vous allez supprimer de façon permanente le pool de clone lié de View Manager. Si les postes de travail liés sont configurés avec des disques persistants, vous pouvez déconnecter ou supprimer ces disques.

c Cliquez sur **[OK]** .

Les machines virtuelles sont supprimées de vCenter Server. De plus, les entrées de base de données View Composer associées et les réplicas créés par View Composer sont supprimés.

d Répétez ces étapes pour chaque pool de clone lié créé par View Composer.

2 Cliquez sur **[View Configuration (Configuration de View)] > [Servers (Serveurs)]** .

3 Dans l'onglet des serveurs vCenter Server, sélectionnez l'instance de vCenter Server à laquelle View Composer est associé.

4 Cliquez sur **[Edit (Modifier)]** .

5 Dans les paramètres de Serveur View Composer, cliquez sur **[Edit (Modifier)]** , sélectionnez **[Do not use View Composer (Ne pas utiliser View Composer)]** et cliquez sur **[OK]** .

Vous ne pouvez plus créer de postes de travail de clone lié dans cette instance de vCenter Server, mais vous pouvez continuer à créer et à gérer des pools de postes de travail de machine virtuelle complets dans l'instance de vCenter Server.

Suivant

Si vous envisagez d'installer View Composer sur un autre hôte et de reconfigurer View Manager pour vous connecter au nouveau service View Composer, vous devez exécuter certaines étapes supplémentaires. Reportez-vous à la section « Migrer View Composer sans poste de travail de clone lié », page 418.

Conflit d'ID uniques de vCenter Server

Si vous possédez plusieurs instances de vCenter Server configurées dans votre environnement, une tentative d'ajout d'une nouvelle instance peut échouer à cause d'un conflit d'ID uniques.

Problème

Vous essayez d'ajouter une instance de vCenter Server à View Manager, mais l'ID unique de l'instance de vCenter Server entre en conflit avec une instance existante.

Cause

Deux instances de vCenter Server ne peuvent pas utiliser le même ID unique. Par défaut, un ID unique de vCenter Server est généré de manière aléatoire, mais vous pouvez le modifier.

Solution

1 Dans vSphere Client, cliquez sur **[Administration] > [vCenter Server Settings (Paramètres de vCenter Server)] > [Runtime Settings (Paramètres d'exécution)]** .

2 Saisissez un nouvel ID unique et cliquez sur **[OK]** .

Pour plus d'informations sur la modification de valeurs d'ID uniques de vCenter Server, consultez la documentation de vSphere.

Sauvegarde de View Connection Server

Après avoir terminé la configuration initiale de View Connection Server, vous pouvez planifier des sauvegardes régulières de vos données de configuration de View Manager et de View Composer.

Pour plus d'informations sur la sauvegarde et la restauration de votre configuration de View, reportez-vous à la section « Sauvegarde et restauration de données de configuration de View », page 403.

Configuration de paramètres pour des sessions client

Vous pouvez définir des paramètres globaux qui affectent les sessions et les connexions client gérées par une instance de Serveur de connexion View ou un groupe répliqué. Vous pouvez définir le délai d'attente de session, afficher des messages de pré-ouverture de session et d'avertissement et spécifier des options de connexion client associées à la sécurité.

Configurer des options pour les sessions et connexions client

Vous configurez des paramètres généraux pour déterminer la façon dont les sessions et les connexions client fonctionnent.

Les paramètres généraux ne sont pas spécifiques à une instance de Serveur de connexion View. Ils affectent toutes les sessions client gérées par une instance de Serveur de connexion View autonome ou un groupe d'instances répliquées.

Vous pouvez également configurer des instances de Serveur de connexion View afin qu'elle utilisent des connexions directes hors tunnel entre des clients View Client et des postes de travail View. Reportez-vous à la section « Configurer le tunnel sécurisé et PCoIP Secure Gateway », page 33 pour plus d'informations sur la configuration de connexions directes.

Prérequis

Familiarisez-vous avec les paramètres généraux. Reportez-vous aux sections « Paramètres généraux pour des sessions client », page 29 et« Paramètres de sécurité globaux pour les sessions et connexions client », page 31.

Procédure

1 Dans View Administrator, cliquez sur **[View Configuration (Configuration de View)] > [Global Settings (Paramètres généraux)]** .

2 Déterminez si vous voulez définir des paramètres généraux ou des paramètres de sécurité.

Option	Description
Paramètres globaux généraux	Dans le volet General (Général), cliquez sur **[Edit (Modifier)]** .
Paramètres de sécurité globaux	Dans le volet Security (Sécurité), cliquez sur **[Edit (Modifier)]** .

3 Configurez les paramètres généraux.

4 Cliquez sur **[OK]** .

Suivant

Vous pouvez changer le mot de passe de la récupération des données fourni au cours de l'installation. Reportez-vous à la section « Changer le mot de passe de la récupération des données », page 28.

Changer le mot de passe de la récupération des données

Vous fournissez un mot de passe de récupération des données lorsque vous installez View Serveur de connexion version 5.1 ou une version supérieure. Après l'installation, vous pouvez changer le mot de passe dans View Administrator. Le mot de passe est nécessaire pour restaurer la configuration View LDAP depuis une sauvegarde.

Lorsque vous sauvegardez Serveur de connexion View, la configuration View LDAP est exportée comme données cryptées LDIF. Pour restaurer la configuration View sauvegardée cryptée, vous devez fournir le mot de passe de récupération.

Le mot de passe doit contenir entre 1 et 128 caractères. Suivez les meilleures pratiques de votre entreprise pour générer des mots de passe sécurisés.

Procédure

1 Dans View Administrator, cliquez sur **[View Configuration (Configuration de View)] > [Global Settings (Paramètres généraux)]** .

2 Dans le volet de sécurité, cliquez sur **[Change data recovery password (Modifier le mot de passe de récupération de données)]** .

3 Tapez deux fois le nouveau mot de passe.

4 (Facultatif) Tapez un rappel de mot de passe.

Remarque Vous pouvez également changer le mot de passe de récupération des données lorsque vous planifiez les données de configuration View à sauvegarder. Reportez-vous à la section « Planifier des sauvegardes de configuration de View Manager », page 404.

Suivant

Lorsque vous utilisez l'outil `vdmimport` pour restaurer une configuration de sauvegarde View, fournissez le nouveau mot de passe.

Paramètres généraux pour des sessions client

Les paramètres généraux déterminent les délais d'expiration de la session, les limites d'activation et du délai d'expiration SSO, les mises à jour d'état dans View Administrator et si des messages de pré-ouverture de session et d'avertissement sont affichés.

Tableau 1-3. Paramètres généraux pour des sessions client

Paramètre	Description
[Délai d'expiration de la session]	Détermine la durée pendant laquelle un utilisateur peut garder une session ouverte après l'ouverture de session sur Serveur de connexion View. La valeur est définie en minutes. Vous devez saisir une valeur. La valeur par défaut est de 600 minutes. Lorsqu'une session de poste de travail expire, la session est terminée et le client View est déconnecté du poste de travail. Cette valeur détermine la durée pendant laquelle une session View Client peut rester connectée à un poste de travail. Cela n'affecte pas la durée pendant laquelle une session Windows est exécutée sur une machine virtuelle de poste de travail.
[authentification unique (SSO)]	Détermine si l'authentification unique (SSO) est activée ou désactivée pour les utilisateurs View et définit la limite du délai d'expiration SSO. Lorsque l'authentification unique est effective, lorsqu'un utilisateur ouvre une session sur Serveur de connexion View à partir de View Client, il n'a pas à ouvrir de nouveau une session pour se connecter au poste de travail View. Au cours d'une session de poste de travail, un utilisateur peut quitter le poste de travail, le laisser devenir inactif et revenir sans avoir à se réauthentifier. Ce paramètre a les options suivantes : ■ **[Désactiver après]** . Active l'authentification unique jusqu'à ce que la limite du délai d'expiration spécifiée soit atteinte. Il s'agit de l'option par défaut. Par défaut, les informations d'identification SSO de l'utilisateur ne sont plus valides après 15 minutes. Cette limite du délai d'expiration SSO réduit les risques qu'une autre personne puisse utiliser la session de poste de travail. Vous pouvez modifier la limite du délai d'expiration SSO en tapant une autre valeur dans la zone de texte **[Désactiver après]** . La limite du délai d'expiration est définie en minutes. Le compteur de la limite de temps démarre lorsque l'utilisateur se connecte à Serveur de connexion View. Par exemple, si vous définissez la valeur sur 10 minutes, les informations d'identification SSO de l'utilisateur sont invalidées 10 minutes après la connexion de l'utilisateur à Serveur de connexion View. ■ **[Toujours activé]** . Active l'authentification unique sans limite du délai d'expiration. ■ **[Désactivé]** . Désactive complètement l'authentification unique. Sur des postes de travail distants, une nouvelle limite du délai d'expiration SSO prend effet immédiatement. Vous n'avez pas à redémarrer le service Serveur de connexion View ou l'ordinateur client. Pour les postes de travail exécutés en mode local, reportez-vous à la section « Limites du délai d'expiration SSO et postes de travail en mode local », page 30.

Tableau 1-3. Paramètres généraux pour des sessions client (suite)

Paramètre	Description
[Délai d'expiration de la session de View Administrator]	Détermine la durée pendant laquelle une session View Administrator inactive continue avant d'expirer. IMPORTANT Définir le délai d'expiration de la session View Administrator sur un nombre de minutes élevé augmente le risque d'utilisation non autorisée de View Administrator. Soyez prudent lorsque vous autorisez une session inactive à durer longtemps. Par défaut, le délai d'expiration de la session View Administrator est de 30 minutes. Vous pouvez définir un délai d'expiration de session compris entre 1 et 4 320 minutes (72 heures).
[Activer les mises à jour d'état automatiques]	Détermine si View Manager met à jour le volet d'état général dans le coin supérieur gauche de View Administrator après quelques minutes de manière répétée. La page du tableau de bord de View Administrator est également mise à jour après quelques minutes de manière répétée. Par défaut, ce paramètre n'est pas activé.
[Afficher un message de pré-ouverture de session]	Affiche une clause de non-responsabilité ou un autre message aux utilisateurs de View Client lorsqu'ils ouvrent une session. Saisissez vos informations ou instructions dans la zone de texte dans la boîte de dialogue Paramètres généraux. Pour n'afficher aucun message, ne cochez pas la case.
[Afficher un avertissement avant la fermeture de session forcée]	Affiche un message d'avertissement quand des utilisateurs sont forcés à fermer leur session car une mise à jour planifiée ou immédiate, telle qu'une opération d'actualisation du poste de travail, est sur le point de démarrer. Ce paramètre détermine également le délai restant avant la fermeture de session de l'utilisateur après l'apparition de l'avertissement. Cochez la case pour afficher un message d'avertissement. Saisissez le nombre de minutes d'attente après l'affichage de l'avertissement et avant la fermeture de session de l'utilisateur. La valeur par défaut est de cinq minutes. Saisissez votre message d'avertissement. Vous pouvez utiliser le message par défaut : `Votre poste de travail est planifié pour une mise à jour importante et s'arrêtera dans 5 minutes. Veuillez enregistrer le travail non sauvegardé maintenant.`

Limites du délai d'expiration SSO et postes de travail en mode local

Sur des postes de travail exécutés en mode local, une nouvelle limite du délai d'expiration SSO prend effet la prochaine fois qu'un ordinateur client qui héberge le poste de travail local envoie un message de pulsation à Serveur de connexion View.

Sur les postes de travail View utilisés en mode local, une opération d'emprunt peut durer plus longtemps que la limite du délai d'expiration SSO. Dans ce cas, les informations d'identification SSO de l'utilisateur expirent avant la fin de l'emprunt.

Par exemple, vous pouvez définir la limite du délai d'expiration SSO sur 10 minutes. Un utilisateur peut se connecter à Serveur de connexion View et emprunter un poste de travail. Si l'emprunt prend 20 minutes et que l'utilisateur lance le poste de travail, l'utilisateur doit toujours ouvrir une session manuellement sur le poste de travail, même s'il n'a pas encore ouvert de session de poste de travail. L'authentification unique réussit lorsque l'utilisateur ferme View Client et se reconnecte à Serveur de connexion View.

Un premier emprunt dans un environnement à faible bande passante peut prendre plus de 15 minutes, la limite du délai d'expiration par défaut. Les informations d'identification SSO de l'utilisateur peuvent expirer lors du premier emprunt si la limite du délai d'expiration SSO par défaut est effective.

Paramètres de sécurité globaux pour les sessions et connexions client

Les paramètres de sécurité globaux déterminent si les clients sont réauthentifiés après des interruptions, le mode de sécurité des messages est activé, IPSec est utilisé pour les connexions de Serveur de sécurité et l'authentification unique (SSO) est utilisée pour les opérations de poste de travail local.

SSL est nécessaire pour toutes les connexions View Client et View Administrator à View. Si votre déploiement View utilise des équilibreurs de charge ou d'autres serveurs intermédiaires de client, vous pouvez décharger SSL vers ces serveurs et configurer des connexions non-SSL dans les instances individuelles de Serveur de connexion View et les Serveurs de sécurité. Reportez-vous à la section « Décharger des connexions SSL sur des serveurs intermédiaires », page 36.

Tableau 1-4. Paramètres de sécurité globaux pour les sessions et connexions client

Paramètre	Description
[Authentifier à nouveau les connexions tunnel sécurisées après une interruption de réseau]	Détermine si les informations d'identification d'utilisateur doivent être réauthentifiées après une interruption de réseau lorsque des clients View Client utilisent des connexions tunnel sécurisées vers des postes de travail View. Lorsque vous sélectionnez ce paramètre, si une connexion tunnel sécurisée se termine au cours d'une session de poste de travail, View Client demande à l'utilisateur de se réauthentifier avant la reconnexion. Ce paramètre renforce la sécurité. Par exemple, si un ordinateur portable est volé et transféré vers un réseau différent, l'utilisateur ne peut pas accéder automatiquement au poste de travail distant, car la connexion réseau est temporairement interrompue. Lorsque ce paramètre n'est pas sélectionné, le client se reconnecte au poste de travail sans demander à l'utilisateur de se réauthentifier. Ce paramètre n'a pas d'effet lorsque vous utilisez une connexion directe.
[Message security mode (Mode de sécurité des messages)]	Détermine si la signature et la vérification des messages JMS transmis entre les composants View Manager ont lieu. Pour plus d'informations, reportez-vous à la section « Mode de sécurité des messages des composants View », page 32. Par défaut, le mode de sécurité des messages est activé.

Tableau 1-4. Paramètres de sécurité globaux pour les sessions et connexions client (suite)

Paramètre	Description
[Use IPSec for Security Server connections (Utiliser IPSec pour les connexions Serveur de sécurité)]	Indique si IPSec (Internet Protocol Security) doit être utilisé pour les connexions entre les Serveurs de sécurité et les instances de Serveur de connexion View . Par défaut, les connexions sécurisées (en utilisant IPSec) pour les connexions de Serveur de sécurité sont activées.
[Disable Single Sign-on for Local Mode operations (Désactiver l'authentification unique pour les opérations en mode local)]	Détermine si l'authentification unique est activée lorsque des utilisateurs ouvrent une session sur leurs postes de travail locaux. Si vous désactivez ce paramètre, les utilisateurs doivent ouvrir une session manuellement sur leurs postes de travail pour démarrer leurs sessions Windows après l'ouverture de session. Quand vous modifiez ce paramètre, la modification prend effet pour chaque utilisateur lors de la prochaine opération de l'utilisateur.

Remarque Si vous effectuez une mise à niveau vers View 5.1 ou une version supérieure depuis une version antérieure de View, le paramètre global **[Require SSL for client connections (SSL requis pour les connexions client et View Administrator)]** s'affiche dans View Administrator, mais uniquement si le paramètre a été désactivé dans la configuration View avant la mise à niveau. Comme SSL est nécessaire pour toutes les connexions View Client et View Administrator à View, ce paramètre ne s'affiche pas dans les nouvelles installations de View 5.1 ou versions suivantes et il n'apparaît pas après une mise à niveau s'il a été activé dans la configuration précédente de View.

Après une mise à niveau, si vous n'activez pas le paramètre **[Require SSL for client connections (SSL requis pour les connexions client et View Administrator)]** , les connexions HTTPS depuis les clients View Client échouent s'ils ne se connectent pas à un périphérique intermédiaire qui est configuré pour établir des connexions directes en utilisant HTTP. Reportez-vous à la section « Décharger des connexions SSL sur des serveurs intermédiaires », page 36.

Mode de sécurité des messages des composants View

Vous pouvez définir un mode de sécurité des messages pour les composants View. Ce paramètre détermine le traitement des signatures des expéditeurs dans les messages JMS. Par défaut, les messages JMS sont rejetés si la signature est absente ou non valide ou qu'un message a été modifié après avoir été signé.

Si un composant dans l'environnement View est antérieur à View Manager 3.0, version dans laquelle la sécurité des messages a été introduite, vous pouvez changer le mode pour consigner un avertissement si ces conditions sont détectées ou ne pas vérifier les signatures du tout. Ces options ne sont pas conseillées et il est préférable de mettre à jour les anciens composants.

Certains messages JMS sont cryptés, car ils contiennent des informations sensibles, telles que les données d'identification de l'utilisateur. Utilisez IPSec pour crypter tous les messages JMS entre les instances de Serveur de connexion View et entre les instances de Serveur de connexion View et les Serveurs de sécurité.

Tableau 1-5 montre les options que vous pouvez sélectionner pour configurer le mode de sécurité des messages. Pour définir une option, sélectionnez-la dans la liste **[Message security mode (Mode de sécurité des messages)]** dans la boîte de dialogue Global Settings (Paramètres généraux).

Tableau 1-5. Options du mode de sécurité des messages

Option	Description
[Disabled (Désactivé)]	Le mode de sécurité des messages est désactivé.
[Mixed (Mélangé)]	Le mode de sécurité des messages est activé mais pas appliqué. Vous pouvez utiliser ce mode pour détecter des composants de votre environnement View qui précèdent View Manager 3.0. Les fichiers journaux générés par Serveur de connexion View contiennent des références à ces composants.
[Enabled (Activé)]	Le mode de sécurité des messages est activé. Les messages non signés sont rejetés par les composants View. Le mode de sécurité des messages est activé par défaut. **Remarque** Les composants View qui précèdent View Manager 3.0 ne sont pas autorisés à communiquer avec d'autres composants View.

La première fois que vous installez View sur un système, le mode de sécurité des messages est **[activé]** par défaut. Si vous mettez à niveau View, le paramètre du mode de sécurité des messages ne change pas.

Le mode de sécurité des messages est pris en charge dans View Manager 3.0 et supérieur. Si vous modifiez le mode de sécurité des messages de **[Disabled (Désactivé)]** ou **[Mixed (Mélangé)]** à **[Enabled (Activé)]**, vous ne pouvez pas lancer un poste de travail avec View Agent depuis Virtual Desktop Manager version 2.1 ou antérieure. Si vous modifiez ensuite le mode de sécurité des messages de **[Enabled (Activé)]** à **[Mixed (Mixe)]** ou **[Disabled (Désactivé)]**, le poste de travail ne parvient toujours pas à démarrer. Pour lancer un poste de travail après avoir modifié le mode de sécurité des messages de **[Enabled (Activé)]** à **[Mixed (Mixe)]** ou **[Disabled (Désactivé)]**, vous devez redémarrer le poste de travail.

Si vous prévoyez de modifier un environnement View actif de **[Disabled (Désactivé)]** à **[Enabled (Activé)]**, ou de **[Enabled (Activé)]** à **[Disabled (Désactivé)]**, passez au mode **[Mixed (Mixe)]** pendant un court moment pour pouvoir faire la modification finale. Par exemple, si votre mode actuel est **[Disabled (Désactivé)]**, passez au mode **[Mixed (Mixe)]** pendant une journée, puis passez à **[Enabled (Activé)]**. En mode **[Mixed (Mixe)]**, les signatures sont jointes aux messages mais ne sont pas vérifiées, ce qui permet de propager la modification du mode des messages dans l'environnement.

Configurer le tunnel sécurisé et PCoIP Secure Gateway

Lorsque le tunnel sécurisé est activé, View Client effectue une deuxième connexion HTTPS avec l'hôte de Serveur de connexion View ou du serveur de sécurité lorsque des utilisateurs se connectent à un poste de travail View.

Lorsque PCoIP Secure Gateway est activé, View Client effectue une autre connexion sécurisée avec l'hôte de Serveur de connexion View ou du serveur de sécurité lorsque des utilisateurs se connectent à un poste de travail View avec le protocole d'affichage PCoIP.

Lorsque le tunnel sécurisé ou PCoIP Secure Gateway n'est pas activé, la session de poste de travail est établie directement entre le système client et la machine virtuelle de poste de travail View, en outrepassant l'hôte de Serveur de connexion View ou du serveur de sécurité. Ce type de connexion est appelé connexion directe.

Important Une configuration de réseau classique pouvant fournir des connexions sécurisées à des clients externes inclut un serveur de sécurité. Pour utiliser View Administrator afin d'activer ou de désactiver le tunnel sécurisé et PCoIP Secure Gateway sur un serveur de sécurité, vous devez modifier l'instance de Serveur de connexion View couplée avec le serveur de sécurité.

Dans une configuration de réseau dans laquelle des clients externes se connectent directement à un hôte de Serveur de connexion View, vous activez ou désactivez le tunnel sécurisé et PCoIP Secure Gateway en modifiant cette instance de Serveur de connexion View dans View Administrator.

Prérequis

- Si vous prévoyez d'activer le composant PCoIP Secure Gateway, vérifiez que l'instance de Serveur de connexion View et que le serveur de sécurité couplé sont View 4.6 ou supérieur.
- Si vous couplez un serveur de sécurité avec une instance de Serveur de connexion View sur laquelle vous avez déjà activé le composant PCoIP Secure Gateway, vérifiez que le serveur de sécurité est View 4.6 ou supérieur.

Procédure

1 Dans View Administrator, cliquez sur **[Configuration de View] > [Serveurs]** .

2 Dans le volet Serveur de connexion View, sélectionnez l'instance de Serveur de connexion View et cliquez sur **[Modifier]** .

3 Configurez l'utilisation du tunnel sécurisé.

Option	Description
Activer le tunnel sécurisé	Cochez la case **[Utiliser une connexion par tunnel sécurisé vers le poste de travail]** .
Désactiver le tunnel sécurisé	Décochez la case **[Utiliser une connexion par tunnel sécurisé vers le poste de travail]** .

Le tunnel sécurisé est activé par défaut.

4 Configurez l'utilisation de PCoIP Secure Gateway.

Option	Description
Activer PCoIP Secure Gateway	Cochez la case **[Utiliser des connexions PCoIP Secure Gateway pour PCoIP vers le poste de travail]** .
Désactiver PCoIP Secure Gateway	Décochez la case **[Utiliser des connexions PCoIP Secure Gateway pour PCoIP vers le poste de travail]** .

PCoIP Secure Gateway est désactivé par défaut.

5 Cliquez sur **[OK]** pour enregistrer vos modifications.

Configurer un accès HTML sécurisé

Dans View Administrator, vous pouvez configurer l'utilisation de Blast Secure Gateway afin de fournir un accès HTML sécurisé à des postes de travail View.

Vous pouvez fournir des connexions sécurisées aux utilisateurs externes qui utilisent HTML Access pour se connecter à des postes de travail View. Blast Secure Gateway, activé par défaut sur les hôtes de Serveur de connexion View et du serveur de sécurité, garantit que seuls les utilisateurs authentifiés peuvent communiquer avec des postes de travail View. Avec HTML Access, le logiciel View Client n'a pas à être installé sur les périphériques de point de terminaison des utilisateurs.

Lorsque Blast Secure Gateway n'est pas activé, les navigateurs Web clients utilisent HTML Access pour établir des connexions directes avec des machines virtuelles de poste de travail View, en outrepassant Blast Secure Gateway.

IMPORTANT Une configuration de réseau classique pouvant fournir des connexions sécurisées à des utilisateurs externes inclut un serveur de sécurité. Pour activer ou désactiver Blast Secure Gateway sur un serveur de sécurité, vous devez modifier l'instance de Serveur de connexion View couplée avec le serveur de sécurité. Si des utilisateurs externes se connectent directement à un hôte de Serveur de connexion View, vous activez ou désactivez Blast Secure Gateway en modifiant cette instance de Serveur de connexion View.

Prérequis

- Si des utilisateurs sélectionnent des postes de travail View à l'aide d'Horizon User Portal, vérifiez qu'Horizon Workspace est installé et configuré pour être utilisé avec Serveur de connexion View et que Serveur de connexion View est couplé avec un serveur d'authentification SAML 2.0.
- Vérifiez que le tunnel sécurisé est activé. S'il est désactivé, Blast Secure Gateway ne peut pas être activé.

Procédure

1 Dans View Administrator, sélectionnez **[Configuration de View] > [Serveurs]** .

2 Dans le volet Serveur de connexions View, sélectionnez l'instance de Serveur de connexion View et cliquez sur **[Modifier]** .

3 Configurez l'utilisation de Blast Secure Gateway.

Option	Description
Activer Blast Secure Gateway	Cochez la case **[Utiliser Blast Secure Gateway pour un accès HTML au poste de travail]**
Désactiver Blast Secure Gateway	Décochez la case **[Utiliser Blast Secure Gateway pour un accès HTML au poste de travail]**

Blast Secure Gateway est activé par défaut.

4 Cliquez sur **[OK]** pour enregistrer vos modifications.

Ouvrir le port utilisé par HTML Access sur des serveurs de sécurité

Lorsque vous installez Serveur de connexion View ou un serveur de sécurité, le programme d'installation de View Server crée la règle de Pare-feu Windows pour le port utilisé par HTML Access pour les connexions client, mais il laisse la règle désactivée tant qu'elle n'est pas réellement nécessaire. Lorsque vous installez ultérieurement HTML Access sur une instance de Serveur de connexion View, le programme d'installation HTML Access active automatiquement la règle pour autoriser la communication avec ce port. Toutefois, sur les serveurs de sécurité, vous devez activer manuellement la règle dans le Pare-feu Windows pour autoriser la communication avec le port.

Par défaut, HTML Access utilise le port TCP 8443 pour les connexions client avec Blast Secure Gateway.

Procédure

- Pour ouvrir le port utilisé par HTML Access sur un ordinateur Serveur de connexion View, installez HTML Access sur cet ordinateur.

  Le programme d'installation HTML Access active la règle **[Serveur de connexion VMware View (Blast-In)]** dans le Pare-feu Windows.

- Pour ouvrir le port pour HTML Access sur un serveur de sécurité, activez manuellement la règle **[Serveur de connexion VMware View (Blast-In)]** dans le Pare-feu Windows.

Décharger des connexions SSL sur des serveurs intermédiaires

Les View Client doivent utiliser HTTPS pour se connecter à View Manager. Si vos View Client se connectent à des équilibreurs de charge ou d'autres serveurs intermédiaires qui transmettent les connexions à des instances de Serveur de connexion View ou à des serveurs de sécurité, vous pouvez décharger SSL vers les serveurs intermédiaires.

Importer des certificats de serveurs de déchargement SSL vers des serveurs View Server

Si vous déchargez des connexions SSL vers un serveur intermédiaire, vous devez importer le certificat du serveur intermédiaire vers les instances de Serveur de connexion View ou les serveurs de sécurité qu'il est en train de décharger. Le même certificat de serveur SSL doit résider sur le serveur intermédiaire de déchargement et sur les serveurs View Server déchargés.

Si le certificat du serveur intermédiaire n'est pas installé sur l'instance de Serveur de connexion View ou sur le serveur de sécurité, les View Client ne peuvent pas valider leurs connexions à View. Dans ce cas, l'empreinte numérique du certificat envoyée par View Server ne correspond pas au certificat sur le serveur intermédiaire auquel les View Client sont connectés.

Ne confondez pas équilibrage de charge et déchargement SSL. L'exigence précédente s'applique à tout périphérique configuré pour fournir le déchargement SSL, y compris certains types d'équilibreurs de charge. Toutefois, l'équilibrage de charge pur ne requiert pas la copie de certificats entre périphériques.

Pour plus d'informations sur l'importation de certificats vers des serveurs View Server, consultez la section « Importer un certificat de serveur signé dans un magasin de certificats Windows » dans le document *Installation de VMware Horizon View*.

Définir des URL externes de View Server pour pointer les clients vers des serveurs de déchargement SSL

Si SSL est déchargé vers un serveur intermédiaire et que des View Client utilisent le tunnel sécurisé pour se connecter à View, veillez à définir l'URL externe du tunnel sécurisé sur une adresse que les clients peuvent utiliser pour accéder au serveur intermédiaire. Si des View Client utilisent PCoIP Secure Gateway, définissez l'URL externe du tunnel sécurisé et l'URL externe PCoIP sur des adresses qui permettent aux clients de se connecter au serveur intermédiaire.

Vous configurez les paramètres d'URL externe sur l'instance de Serveur de connexion View ou sur le serveur de sécurité qui se connecte au serveur intermédiaire. Pour plus d'informations, consultez la section « Configuration d'URL externes pour PCoIP Secure Gateway et les connexions par tunnel » dans le document *Installation de VMware Horizon View*.

Autoriser les connexions HTTP aux serveurs intermédiaires

Lorsque SSL est déchargé vers un serveur intermédiaire, vous pouvez configurer les instances de Serveur de connexion View ou les Serveurs de sécurité pour autoriser les connexions HTTP depuis les périphériques client intermédiaires. Les périphériques intermédiaires doivent accepter HTTPS pour les connexions View Client.

Pour autoriser les connexions HTTP entre les View servers et les périphériques intermédiaires, vous devez configurer le fichier `locked.properties` sur chaque instance de Serveur de connexion View et chaque Serveur de sécurité sur lesquels les connexions HTTP sont autorisées.

Même lorsque les connexions HTTP entre les View servers et les périphériques intermédiaires sont autorisées, vous ne pouvez pas désactiver SSL dans View. Les View servers continuent d'accepter les connexions HTTPS et les connexions HTTP.

Remarque Si les clients View Client utilisent l'authentification par carte à puce, ils doivent établir des connexions HTTPS directement à Serveur de connexion View ou au Serveur de sécurité. Le déchargement SSL n'est pas pris en charge avec l'authentification par carte à puce.

Procédure

1 Créez ou modifiez le fichier `locked.properties` dans le dossier de configuration de la passerelle SSL sur l'hôte de Serveur de connexion View ou du Serveur de sécurité.

   Par exemple : *`install_directory`*`\VMware\VMware View\Server\sslgateway\conf\locked.properties`

2 Pour configurer le protocole de View server, ajoutez la propriété `serverProtocol` et affectez-lui la valeur `http`.

   La valeur `http` doit être entrée en minuscules.

3 (Facultatif) Ajoutez des propriétés pour configurer un port d'écoute HTTP autre que par défaut et une interface réseau sur View server.

   - Pour remplacer le port d'écoute HTTP 80, affectez à `serverPortNonSSL` un autre numéro de port auquel le périphérique intermédiaire doit se connecter.
   - Si le View server dispose de plusieurs interfaces réseau et que vous voulez que le serveur écoute les connexions HTTP sur une seule interface, affectez à `serverHost` l'adresse IP de cette interface réseau.

4 Enregistrez le fichier `locked.properties`.

5 Redémarrez le service Serveur de connexion View ou le service du Serveur de sécurité pour que vos modifications prennent effet.

Exemple : fichier locked.properties

Ce fichier permet les connexions HTTP non-SSL à un View server. L'adresse IP de l'interface réseau client du View server est 10.20.30.40. Le serveur utilise le port par défaut 80 pour écouter les connexions HTTP. La valeur `http` doit être en minuscules.

```
serverProtocol=http
serverHost=10.20.30.40
```

Désactiver ou activer View Connection Server

Vous pouvez désactiver une instance de View Connection Server pour empêcher les utilisateurs d'ouvrir une session sur leurs postes de travail View. Après avoir désactivé une instance, vous pouvez l'activer de nouveau.

Lorsque vous désactivez une instance de View Connection Server, les utilisateurs actuellement connectés à des postes de travail View ne sont pas affectés.

Votre déploiement de View Manager détermine comment les utilisateurs sont affectés en désactivant une instance.

- S'il s'agit d'une instance autonome de View Connection Server, les utilisateurs ne peuvent pas ouvrir de session sur leurs postes de travail. Ils ne peuvent pas se connecter à View Connection Server.
- S'il s'agit d'une instance de View Connection Server répliquée, votre topologie de réseau détermine si les utilisateurs peuvent être routés vers une autre instance répliquée. Si des utilisateurs peuvent accéder à une autre instance, ils peuvent ouvrir une session sur leurs postes de travail.

Procédure

1 Dans View Administrator, cliquez sur **[View Configuration (Configuration de View)] > [Servers (Serveurs)]** .

2 Dans le volet View Connection Servers (Serveurs View Connection Server), sélectionnez l'instance de View Connection Server.

3 Cliquez sur **[Disable (Désactiver)]** .

Vous pouvez activer de nouveau l'instance en cliquant sur **[Enable (Activer)]** .

Modifier les URL externes

Vous pouvez utiliser View Administrator pour modifier des URL externes pour des instances de Serveur de connexion View et des serveurs de sécurité.

Par défaut, un hôte de Serveur de connexion View ou d'un serveur de sécurité ne peut être contacté que par des clients tunnel qui résident sur le même réseau. Les clients tunnel qui s'exécutent en dehors de votre réseau doivent utiliser une URL résolvable par client pour se connecter à un hôte de Serveur de connexion View ou du serveur de sécurité.

Lorsque des utilisateurs se connectent à des postes de travail View avec le protocole d'affichage PCoIP, View Client peut réaliser une autre connexion à PCoIP Secure Gateway sur l'hôte de Serveur de connexion View ou du serveur de sécurité. Pour utiliser PCoIP Secure Gateway, un système client doit avoir accès à une adresse IP autorisant le client à atteindre l'hôte de Serveur de connexion View ou du serveur de sécurité. Vous spécifiez cette adresse IP dans l'URL externe PCoIP.

L'URL externe de tunnel sécurisé et l'URL externe PCoIP doivent être les adresses que les systèmes client utilisent pour atteindre cet hôte. Par exemple, si vous configurez un hôte de Serveur de connexion View, ne spécifiez pas l'URL externe du tunnel sécurisé pour cet hôte et l'URL externe PCoIP pour un serveur de sécurité couplé.

Remarque Vous ne pouvez pas modifier les URL externes pour un serveur de sécurité qui n'a pas été mis à niveau vers Serveur de connexion View 4.5 ou supérieur.

Procédure

1 Dans View Administrator, cliquez sur **[View Configuration (Configuration de View)] > [Servers (Serveurs)]** .

Option	Action
Instance de Serveur de connexion View	Sélectionnez l'instance de Serveur de connexion View dans le volet View Connection Servers (Serveurs de connexion View) et cliquez sur **[Edit (Modifier)]** .
Serveur de sécurité	Sélectionnez le serveur de sécurité dans le volet Security Servers (Serveurs de sécurité) et cliquez sur **[Edit (Modifier)]** .

2 Saisissez l'URL externe du tunnel sécurisé dans la zone de texte **[External URL (URL externe)]** .

L'adresse URL doit contenir le protocole, le nom d'hôte résolvable par le client et le numéro de port.

Par exemple : https://view.exemple.com:443

Remarque Vous pouvez utiliser l'adresse IP si vous avez accès à une instance de Serveur de connexion View ou un serveur de sécurité lorsque le nom d'hôte n'est pas résolvable. Cependant, l'hôte que vous contactez ne fera pas correspondre le certificat SSL configuré pour l'instance Serveur de connexion View ou le serveur de sécurité, ce qui bloque l'accès ou génère un accès avec une sécurité réduite.

3 Saisissez l'URL externe de PCoIP Secure Gateway dans la zone de texte **[PCoIP External URL (URL externe PCoIP)]** .

Spécifiez l'URL externe PCoIP comme adresse IP avec le numéro de port 4172. N'incluez pas un nom de protocole.

Par exemple : `10.20.30.40:4172`

L'URL doit contenir l'adresse IP et le numéro de port qu'un système client peut utiliser pour atteindre cette instance de serveur de sécurité ou de Serveur de connexion View. Vous ne pouvez saisir du texte dans la zone de texte que si PCoIP Secure Gateway est installé sur l'instance de serveur de sécurité ou de Serveur de connexion View.

4 Cliquez sur **[OK]** pour enregistrer vos modifications.

Les URL externes sont mises à jour immédiatement. Vous n'avez pas à redémarrer le service Serveur de connexion View ou le service du serveur de sécurité pour que les modifications prennent effet.

Participer ou se retirer du programme d'amélioration de l'expérience du client

Lorsque vous installez Serveur de connexion View avec une nouvelle configuration, vous pouvez décider de participer à un programme d'amélioration de l'expérience du client. Si vous changez d'avis sur votre participation après l'installation, vous pouvez participer ou ne plus participer au programme en utilisant View Administrator.

Si vous participez au programme, VMware collecte des données anonymes sur votre déploiement afin d'améliorer la réponse de VMware aux besoins du client. Aucune donnée identifiant votre entreprise n'est collectée.

Pour vérifier la liste des champs dont les données sont collectées, y compris les champs rendus anonymes, voir « Informations collectées par le programme d'amélioration de l'expérience du client », page 422.

Procédure

1 Dans View Administrator, cliquez sur **[View Configuration (Configuration de View)] > [Product licensing and usage (Licence produit et utilisation)]** .

2 Dans le volet du programme de l'expérience du client, cliquez sur **[Edit (Modifier)]** .

3 Indiquez que vous voulez participer ou ne plus participer au programme en cochant ou en désélectionnant la case **[Send anonymous data to VMware (Envoyer des données anonymes à VMware)]** .

4 (Facultatif) Si vous participez, vous pouvez sélectionner l'emplacement géographique, le type d'entreprise et le nombe d'employés de votre entreprise.

5 Cliquez sur **[OK]** .

Répertoire View LDAP

View LDAP est le répertoire de données pour toutes les informations de configuration de View Manager. View LDAP est un répertoire LDAP (Lightweight Directory Access Protocol) incorporé fourni avec l'installation de View Connection Server.

View LDAP contient les composants de répertoire LDAP standard utilisés par View Manager.

- des définitions de schémas de View Manager ;
- des définitions de DIT (Directory Information Tree) ;
- des listes de contrôle d'accès (ACL).

View LDAP contient des entrées de répertoire qui représentent des objets View Manager.

- Des entrées de poste de travail View qui représentent chaque poste de travail accessible. Chaque entrée contient des références aux entrées de sécurité extérieure principale d'utilisateurs et de groupes de Windows dans Active Directory qui sont autorisés à utiliser le poste de travail.
- Des entrées de pool de postes de travail View qui représentent plusieurs postes de travail virtuels gérés ensemble.
- Des entrées de machine virtuelle qui représentent la machine virtuelle vCenter Server pour chaque poste de travail.
- Des entrées de composant View Manager qui stockent des paramètres de configuration.

View LDAP contient également un ensemble de DLL de plug-in de View Manager qui fournissent des services d'automatisation et de notification pour d'autres composants View Manager.

Remarque Les instances de serveur de sécurité ne contiennent pas de répertoire View LDAP.

Configuration d'administration déléguée basée sur des rôles 2

Une tâche de gestion clé dans un environnement View consiste à déterminer qui peut utiliser View Administrator et les tâches que ces utilisateurs sont autorisés à effectuer. Avec l'administration déléguée basée sur des rôles, vous pouvez affecter de façon sélective des droits d'administration en affectant des rôles d'administrateur à des utilisateurs et des groupes Active Directory spécifiques.

Ce chapitre aborde les rubriques suivantes :

Comprendre les rôles et les privilèges

La possibilité d'effectuer des tâches dans View Administrator est déterminée par un système de contrôle d'accès composé de rôles et de privilèges d'administrateur. Ce système est similaire au système de contrôle d'accès du vCenter Server.

Un rôle d'administrateur est un ensemble de privilèges. Les privilèges accordent la possibilité d'effectuer des actions spécifiques, comme autoriser un utilisateur sur un pool de postes de travail. Les privilèges contrôlent également ce qu'un administrateur peut voir dans View Administrator. Par exemple, si un administrateur ne dispose pas de privilèges pour voir ou modifier des règles générales, le paramètre **[Global Policies (Règles générales)]** n'est pas visible dans le volet de navigation lorsque l'administrateur ouvre une session sur View Administrator.

Les privilèges d'administrateur sont généraux ou spécifiques de l'objet. Les privilèges généraux contrôlent les opérations système, telles que l'affichage et la modification des paramètres généraux. Les privilèges spécifiques de l'objet contrôlent les opérations sur des types spécifiques d'objets d'inventaire.

Les rôles d'administrateur combinent généralement tous les privilèges individuels requis pour effectuer une tâche d'administration à un niveau supérieur. View Administrator comporte des rôles prédéfinis qui contiennent les privilèges requis pour effectuer des tâches d'administration habituelles. Vous pouvez affecter ces rôles prédéfinis à vos utilisateurs et groupes d'administrateurs, ou vous pouvez créer vos propres rôles en combinant des privilèges sélectionnés. Vous ne pouvez pas modifier les rôles prédéfinis.

Pour créer des administrateurs, vous sélectionnez des utilisateurs et des groupes dans vos utilisateurs et groupes Active Directory et affectez des rôles d'administrateur. Les administrateurs obtiennent des privilèges via leurs affectations de rôle. Vous ne pouvez pas affecter de privilèges directement à des administrateurs. Un administrateur qui a plusieurs affectations de rôle acquiert la somme de tous les privilèges contenus dans ces rôles.

Utilisation de dossiers pour déléguer l'administration

Par défaut, des pools de postes de travail sont créés dans le dossier racine, qui apparaît sous la forme / ou Racine(/) dans View Administrator. Vous pouvez créer des dossiers sous le dossier racine pour subdiviser vos pools de postes de travail et déléguer l'administration de pools de postes de travail spécifiques à différents administrateurs.

Un poste de travail hérite du dossier depuis son pool. Un disque persistant attaché hérite du dossier depuis son poste de travail. Vous pouvez posséder un maximum de 100 dossiers, y compris le dossier racine.

Vous configurez un accès administrateur aux ressources dans un dossier en affectant un rôle à un administrateur sur ce dossier. Les administrateurs ne peuvent accéder qu'aux ressources qui résident dans des dossiers pour lesquels ils ont affecté des rôles. Le rôle qu'un administrateur a sur un dossier détermine son niveau d'accès sur les ressources contenues dans ce dossier.

Comme les rôles sont hérités depuis le dossier racine, un administrateur qui a un rôle sur le dossier racine a ce rôle sur tous les dossiers. Les administrateurs avec le rôle Administrateurs sur le dossier racine sont des super administrateurs car ils ont un accès complet à tous les objets d'inventaire dans le système.

Un rôle doit contenir au moins un privilège spécifique de l'objet pour s'appliquer à un dossier. Les rôles ne contenant que des privilèges généraux ne peuvent pas être appliqués à des dossiers.

Vous pouvez utiliser View Administrator pour créer des dossiers et déplacer des pools existants dans des dossiers. Vous pouvez également sélectionner un dossier lorsque vous créez un pool de postes de travail. Si vous ne sélectionnez pas un dossier au cours de la création d'un pool, le pool est créé dans le dossier racine par défaut.

Remarque Si vous prévoyez de fournir l'accès à vos postes de travail via Horizon Workspace, vérifiez que vous créez les pools de postes de travail en tant qu'utilisateur avec des autorisations Administrateurs dans le dossier racine dans View. Si vous accordez à l'utilisateur des autorisations Administrateurs sur un dossier autre que le dossier racine, Horizon Workspace ne reconnaîtra pas l'authentificateur SAML 2.0 que vous configurez dans View et vous ne pouvez pas configurer le pool dans Horizon Workspace.

Différents administrateurs pour différents dossiers

Vous pouvez créer un administrateur différent pour gérer chaque dossier dans votre configuration.

Par exemple, si vos pools de postes de travail d'entreprise se trouvent dans un dossier et que vos pools de postes de travail pour les développeurs de logiciels se trouvent dans un autre dossier, vous pouvez créer différents administrateurs pour gérer les ressources dans chaque dossier.

Tableau 2-1 montre un exemple de ce type de configuration.

Tableau 2-1. Différents administrateurs pour différents dossiers

Administrateur	Rôle	Dossier
view-domain.com\Admin1	Inventory Administrators (Administrateurs d'inventaire)	`/CorporateDesktops`
view-domain.com\Admin2	Inventory Administrators (Administrateurs d'inventaire)	`/DeveloperDesktops`

Dans cet exemple, l'administrateur Admin1 a le rôle Inventory Administrators (Administrateurs d'inventaire) sur le dossier appelé `CorporateDesktops`, et l'administrateur Admin2 a le rôle Inventory Administrators (Administrateurs d'inventaire) sur le dossier appelé `DeveloperDesktops`..

Différents administrateurs pour le même dossier

Vous pouvez créer différents administrateurs pour gérer le même dossier.

Par exemple, si les pools de postes de travail de votre entreprise se trouvent dans un dossier, vous pouvez créer un administrateur qui peut voir et modifier ces pools et un autre administrateur qui peut uniquement les voir.

Tableau 2-2 montre un exemple de ce type de configuration.

Tableau 2-2. Différents administrateurs pour le même dossier

Administrateur	Rôle	Dossier
view-domain.com\Admin1	Inventory Administrators (Administrateurs d'inventaire)	`/CorporateDesktops`
view-domain.com\Admin2	Inventory Administrators (Read only) (Administrateurs d'inventaire (lecture seule))	`/CorporateDesktops`

Dans cet exemple, l'administrateur Admin1 a le rôle Inventory Administrators (Administrateurs d'inventaire) sur le dossier appelé `CorporateDesktops`, et l'administrateur Admin2 a le rôle Inventory Administrators (Read only) (Administrateurs d'inventaire (lecture seule)) sur le même dossier.

Comprendre les autorisations

Dans View Administrator, une autorisation est la combinaison d'un rôle, d'un utilisateur ou d'un groupe d'administrateurs et d'un dossier. Le rôle définit les actions pouvant être effectuées, l'utilisateur ou le groupe indique qui peut effectuer l'action et le dossier contient les objets qui sont la cible de l'action.

Les autorisations apparaissent différemment dans View Administrator selon que vous sélectionnez un utilisateur ou un groupe d'administrateurs, un dossier ou un rôle.

Tableau 2-3 montre comment les autorisations apparaissent dans View Administrator lorsque vous sélectionnez un utilisateur ou un groupe d'administrateurs. L'utilisateur administrateur est appelé Admin 1 et il possède deux autorisations.

Tableau 2-3. Autorisations sous l'onglet Administrateurs et groupes pour Admin 1

Rôle	Dossier
Inventory Administrators (Administrateurs d'inventaire)	`MarketingDesktops`
Administrators (Read Only) (Administrateurs (lecture seule))	`/`

La première autorisation montre qu'Admin 1 a le rôle Inventory Administrators (Administrateurs d'inventaire) sur le dossier appelé `MarketingDesktops`. La deuxième autorisation montre qu'Admin 1 a le rôle Administrators (Read only) (Administrateurs (lecture seule)) sur le dossier racine.

Tableau 2-4 montre comment les mêmes autorisations apparaissent dans View Administrator lorsque vous sélectionnez le dossier `MarketingDesktops`.

Tableau 2-4. Autorisations sous l'onglet Dossiers pour MarketingDesktops

Admin	Rôle	Héritée
view-domain.com\Admin1	Inventory Administrators (Administrateurs d'inventaire)	
view-domain.com\Admin1	Administrators (Read Only) (Administrateurs (lecture seule))	Oui

La première autorisation est la même que la première autorisation indiquée dans le Tableau 2-3. La deuxième autorisation est héritée de la deuxième autorisation indiquée dans le Tableau 2-3. Comme les dossiers héritent des autorisations du dossier racine, Admin1 a le rôle Administrators (Read only) (Administrateurs (lecture seule)) sur le dossier `MarketingDesktops`. Lorsqu'une autorisation est héritée, Oui apparaît dans la colonne Héritée.

Tableau 2-5 montre comment la première autorisation dans le Tableau 2-3 apparaît dans View Administrator lorsque vous sélectionnez le rôle Inventory Administrators (Administrateurs d'inventaire).

Tableau 2-5. Autorisations sous l'onglet Rôle pour Inventory Administrators (Administrateurs d'inventaire)

Administrateur	Dossier
view-domain.com\Admin1	`/MarketingDesktops`

Gérer des administrateurs

Les utilisateurs qui ont le rôle Administrators peuvent utiliser View Administrator pour ajouter et supprimer des utilisateurs et des groupes d'administrateurs.

Le rôle Administrators est le rôle le plus puissant dans View Administrator. À l'origine, le rôle Administrators est attribué aux membres du compte View Administrators. Vous spécifiez le compte View Administrators lorsque vous installez View Connection Server. Le compte View Administrators peut être le groupe Administrators local (BUILTIN\Administrators) sur l'ordinateur View Connection Server ou un compte d'utilisateur ou de groupe de domaine.

Remarque Par défaut, le groupe Domain Admins est un membre du groupe Administrators local. Si vous avez spécifié le compte View Administrators en tant que groupe Administrators local, et si vous ne voulez pas que des administrateurs de domaine aient un accès complet à des objets d'inventaire et à des paramètres de configuration View, vous devez supprimer le groupe Domain Admins du groupe Administrators local.

- Créer un administrateur page 45

  Pour créer un administrateur, vous sélectionnez un utilisateur ou un groupe parmi vos utilisateurs et groupes Active Directory dans View Administrator et affectez un rôle d'administrateur.

- Supprimer un administrateur page 46

  Vous pouvez supprimer un utilisateur ou un groupe d'administrateurs. Vous ne pouvez pas supprimer le dernier super administrateur dans le système. Un super administrateur est un administrateur qui a le rôle Administrators sur le dossier racine.

Créer un administrateur

Pour créer un administrateur, vous sélectionnez un utilisateur ou un groupe parmi vos utilisateurs et groupes Active Directory dans View Administrator et affectez un rôle d'administrateur.

Prérequis

- Familiarisez-vous avec les rôles d'administrateur prédéfinis. Reportez-vous à la section « Rôles et privilèges prédéfinis », page 52.
- Familiarisez-vous avec les meilleures pratiques pour la création d'utilisateurs et de groupes d'administrateurs. Reportez-vous à la section « Meilleures pratiques pour des utilisateurs et des groupes d'administrateurs », page 59.
- Pour affecter un rôle personnalisé à l'administrateur, créez le rôle personnalisé. Reportez-vous à la section « Ajouter un rôle personnalisé », page 51.
- Pour créer un administrateur pouvant gérer des pools de postes de travail spécifiques, créez un dossier et déplacez les pools de postes de travail vers ce dossier. Reportez-vous à la section « Gérer et consulter des dossiers », page 48.

Procédure

1 Dans View Administrator, sélectionnez **[View Configuration (Configuration de View)] > [Administrators (Administrateurs)]** .

2 Sous l'onglet **[Administrators and Groups (Administrateurs et groupes)]** , cliquez sur **[Add User or Group (Ajouter un utilisateur ou un groupe)]** .

3 Cliquez sur **[Add (Ajouter)]** , sélectionnez un ou plusieurs critères de recherche, puis cliquez sur **[Find (Rechercher)]** pour filtrer des utilisateurs ou des groupes Active Directory en fonction de vos critères de recherche.

4 Sélectionnez l'utilisateur ou le groupe Active Directory auquel vous voulez attribuer le rôle d'administrateur, cliquez sur **[OK]** et sur **[Next (Suivant)]** .

Vous pouvez appuyer sur les touches Ctrl et Maj pour sélectionner plusieurs utilisateurs et groupes.

5 Sélectionnez un rôle à affecter à l'utilisateur ou au groupe d'administrateurs.

La colonne Apply to Folder (Appliquer au dossier) indique si un rôle s'applique à des dossiers. Seuls les rôles contenant des privilèges spécifiques de l'objet s'appliquent à des dossiers. Les rôles ne contenant que des privilèges généraux ne s'appliquent pas à des dossiers.

Option	Action
The role you selected applies to folders (Le rôle que vous avez sélectionné s'applique à des dossiers)	Sélectionnez un ou plusieurs dossiers et cliquez sur **[Next (Suivant)]** .
You want the permission to apply to all folders (Vous voulez l'autorisation d'appliquer à tous les dossiers)	Sélectionnez le dossier racine et cliquez sur **[Next (Suivant)]** .

6 Cliquez sur **[Finish (Terminer)]** pour créer l'utilisateur ou le groupe d'administrateurs.

Le nouvel utilisateur ou groupe d'administrateurs apparaît dans le volet de gauche et le rôle et le dossier que vous avez sélectionnés apparaissent dans le volet de droite sous l'onglet **[Administrators and Groups (Administrateurs et groupes)]** .

Supprimer un administrateur

Vous pouvez supprimer un utilisateur ou un groupe d'administrateurs. Vous ne pouvez pas supprimer le dernier super administrateur dans le système. Un super administrateur est un administrateur qui a le rôle Administrators sur le dossier racine.

Procédure

1 Dans View Administrator, sélectionnez **[View Configuration (Configuration de View)] > [Administrators (Administrateurs)]** .

2 Sous l'onglet **[Administrators and Groups (Administrateurs et groupes)]** , sélectionnez l'utilisateur ou le groupe d'administrateurs, cliquez sur **[Remove User or Group (Supprimer un utilisateur ou un groupe)]** et sur **[OK]** .

L'utilisateur ou le groupe d'administrateurs n'apparaît plus sous l'onglet **[Administrators and Groups (Administrateurs et groupes)]** .

Gérer et consulter des autorisations

Vous pouvez utiliser View Administrator pour ajouter, supprimer et consulter des autorisations pour des utilisateurs et des groupes d'administrateurs spécifiques, des rôles spécifiques et des dossiers spécifiques.

- Ajouter une autorisation page 46

  Vous pouvez ajouter une autorisation qui comporte un utilisateur ou un groupe d'administrateurs spécifique, un rôle spécifique ou un dossier spécifique.

- Supprimer une autorisation page 47

  Vous pouvez supprimer une autorisation qui comporte un utilisateur ou un groupe d'administrateurs spécifique, un rôle spécifique ou un dossier spécifique.

- Consulter des autorisations page 48

  Vous pouvez consulter les autorisations qui comportent un administrateur ou un groupe spécifique, un rôle spécifique ou un dossier spécifique.

Ajouter une autorisation

Vous pouvez ajouter une autorisation qui comporte un utilisateur ou un groupe d'administrateurs spécifique, un rôle spécifique ou un dossier spécifique.

Procédure

1 Dans View Administrator, sélectionnez **[View Configuration (Configuration de View)] > [Administrators (Administrateurs)]** .

2 Créez l'autorisation.

Option	Action
Create a permission that includes a specific administrator user or group (Créer une autorisation qui inclut un utilisateur ou un groupe d'administrateurs spécifique)	a Sous l'onglet **[Administrators and Groups (Administrateurs et groupes)]** , sélectionnez l'administrateur ou le groupe et cliquez sur **[Add Permission (Ajouter une autorisation)]** . b Sélectionnez un rôle. c Si le rôle ne s'applique pas aux dossiers, cliquez sur **[Finish (Terminer)]** . d Si le rôle s'applique à des dossiers, cliquez sur **[Next (Suivant)]** , sélectionnez un ou plusieurs dossiers et cliquez sur **[Finish (Terminer)]** . Un rôle doit contenir au moins un privilège spécifique de l'objet pour s'appliquer à un dossier.
Create a permission that includes a specific role (Créer une autorisation qui inclut un rôle spécifique)	a Sous l'onglet **[Roles (Rôles)]** , sélectionnez le rôle, cliquez sur **[Permissions (Autorisations)]** puis sur **[Add Permission (Ajouter une autorisation)]** . b Cliquez sur **[Add (Ajouter)]** , sélectionnez un ou plusieurs critères de recherche, puis cliquez sur **[Find (Rechercher)]** pour rechercher des utilisateurs ou des groupes d'administrateurs qui correspondent à vos critères de recherche. c Sélectionnez un utilisateur ou un groupe d'administrateurs à inclure dans l'autorisation et cliquez sur **[OK]** . Vous pouvez appuyer sur les touches Ctrl et Maj pour sélectionner plusieurs utilisateurs et groupes. d Si le rôle ne s'applique pas aux dossiers, cliquez sur **[Finish (Terminer)]** . e Si le rôle s'applique à des dossiers, cliquez sur **[Next (Suivant)]** , sélectionnez un ou plusieurs dossiers et cliquez sur **[Finish (Terminer)]** . Un rôle doit contenir au moins un privilège spécifique de l'objet pour s'appliquer à un dossier.
Create a permission that includes a specific folder (Créer une autorisation qui inclut un dossier spécifique)	a Sous l'onglet **[Folders (Dossiers)]** , sélectionnez le dossier et cliquez sur **[Add Permission (Ajouter une autorisation)]** . b Cliquez sur **[Add (Ajouter)]** , sélectionnez un ou plusieurs critères de recherche, puis cliquez sur **[Find (Rechercher)]** pour rechercher des utilisateurs ou des groupes d'administrateurs qui correspondent à vos critères de recherche. c Sélectionnez un utilisateur ou un groupe d'administrateurs à inclure dans l'autorisation et cliquez sur **[OK]** . Vous pouvez appuyer sur les touches Ctrl et Maj pour sélectionner plusieurs utilisateurs et groupes. d Cliquez sur **[Next (Suivant)]** , sélectionnez un rôle et cliquez sur **[Finish (Terminer)]** . Un rôle doit contenir au moins un privilège spécifique de l'objet pour s'appliquer à un dossier.

Supprimer une autorisation

Vous pouvez supprimer une autorisation qui comporte un utilisateur ou un groupe d'administrateurs spécifique, un rôle spécifique ou un dossier spécifique.

Si vous supprimez la dernière autorisation pour un utilisateur ou un groupe d'administrateurs, cet utilisateur ou ce groupe d'administrateurs est également supprimé. Comme au moins un administrateur doit posséder le rôle Administrators sur le dossier racine, vous ne pouvez pas supprimer une autorisation qui entraînerait la suppression de cet administrateur. Vous ne pouvez pas supprimer une autorisation héritée.

Procédure

1 Dans View Administrator, sélectionnez **[View Configuration (Configuration de View)] > [Administrators (Administrateurs)]** .

2 Sélectionnez l'autorisation à supprimer.

Option	Action
Delete a permission that applies to a specific administrator or group (Supprimer une autorisation qui s'applique à un administrateur ou un groupe spécifique)	Sélectionnez l'administrateur ou le groupe sous l'onglet **[Administrators and Groups (Administrateurs et groupes)]** .
Delete a permission that applies to a specific role (Supprimer une autorisation qui s'applique à un rôle spécifique)	Sélectionnez le rôle sous l'onglet **[Roles (Rôles)]** .
Delete a permission that applies to a specific folder (Supprimer une autorisation qui s'applique à un dossier spécifique)	Sélectionnez le dossier sous l'onglet **[Folders (Dossiers)]** .

3 Sélectionnez l'autorisation et cliquez sur **[Delete Permission (Supprimer une autorisation)]** .

Consulter des autorisations

Vous pouvez consulter les autorisations qui comportent un administrateur ou un groupe spécifique, un rôle spécifique ou un dossier spécifique.

Procédure

1 Sélectionnez **[View Configuration (Configuration de View)]** > **[Administrators (Administrateurs)]** .

2 Consultez les autorisations.

Option	Action
Review the permissions that include a specific administrator or group (Consulter les autorisations qui comportent un administrateur ou un groupe spécifique)	Sélectionnez l'administrateur ou le groupe sous l'onglet **[Administrators and Groups (Administrateurs et groupes)]** .
Review the permissions that include a specific role (Consulter les autorisations qui comportent un rôle spécifique)	Sélectionnez le rôle sous l'onglet **[Roles (Rôles)]** et cliquez sur **[Permissions (Autorisations)]** .
Review the permissions that include a specific folder (Consulter les autorisations qui comportent un dossier spécifique)	Sélectionnez le dossier sous l'onglet **[Folders (Dossiers)]** .

Gérer et consulter des dossiers

Vous pouvez utiliser View Administrator pour ajouter et supprimer des dossiers et pour consulter les pools de postes de travail et les postes de travail dans un dossier particulier.

- Ajouter un dossier page 49

  Si vous voulez déléguer l'administration de postes de travail ou de pools spécifiques à différents administrateurs, vous devez créer des dossiers pour subdiviser vos postes de travail ou vos pools. Si vous ne créez pas de dossiers, tous les postes de travail et les pools résident dans le dossier racine.

- Déplacer un pool de postes de travail vers un dossier différent page 49

  Après avoir créé un dossier pour subdiviser vos pools de postes de travail, vous devez déplacer manuellement des pools de postes de travail vers le nouveau dossier. Si vous décidez de modifier le mode de subdivision de vos pools de postes de travail, vous pouvez déplacer des pools de postes de travail d'un dossier à l'autre.

- Supprimer un dossier page 50

  Vous pouvez supprimer un dossier s'il ne contient aucun objet d'inventaire. Vous ne pouvez pas supprimer le dossier racine.

- Consulter les pools de postes de travail dans un dossier page 50

  Vous pouvez voir tous les pools de postes de travail dans un dossier particulier dans View Administrator.

- Consulter les postes de travail dans un dossier page 50

  Vous pouvez voir tous les postes de travail dans un dossier particulier dans View Administrator. Un poste de travail hérite du dossier depuis son pool.

Ajouter un dossier

Si vous voulez déléguer l'administration de postes de travail ou de pools spécifiques à différents administrateurs, vous devez créer des dossiers pour subdiviser vos postes de travail ou vos pools. Si vous ne créez pas de dossiers, tous les postes de travail et les pools résident dans le dossier racine.

Vous pouvez posséder un maximum de 100 dossiers, y compris le dossier racine.

Procédure

1 Dans View Administrator, sélectionnez **[Inventory (Inventaire)] > [Pools]** .

2 Dans le menu déroulant **[Folder (Dossier)]** sur la barre de commande, sélectionnez **[New Folder (Nouveau dossier)]** .

3 Saisissez un nom et une description pour le dossier et cliquez sur **[OK]** .

La description est facultative.

Suivant

Déplacez un ou plusieurs pools de postes de travail vers le dossier.

Déplacer un pool de postes de travail vers un dossier différent

Après avoir créé un dossier pour subdiviser vos pools de postes de travail, vous devez déplacer manuellement des pools de postes de travail vers le nouveau dossier. Si vous décidez de modifier le mode de subdivision de vos pools de postes de travail, vous pouvez déplacer des pools de postes de travail d'un dossier à l'autre.

Procédure

1 Dans View Administrator, sélectionnez **[Inventory (Inventaire)] > [Pools]** et sélectionnez le pool.

2 Dans le menu déroulant **[Folder (Dossier)]** , sélectionnez **[Change Folder (Changer de dossier)]** .

3 Sélectionnez le dossier et cliquez sur **[OK]** .

View Administrator déplace le pool vers le dossier que vous avez sélectionné.

Supprimer un dossier

Vous pouvez supprimer un dossier s'il ne contient aucun objet d'inventaire. Vous ne pouvez pas supprimer le dossier racine.

Prérequis

Si le dossier contient des objets d'inventaire, déplacez les objets vers un autre dossier ou vers le dossier racine. Reportez-vous à la section « Déplacer un pool de postes de travail vers un dossier différent », page 49.

Procédure

1 Dans View Administrator, sélectionnez **[View Configuration (Configuration de View)] > [Administrators (Administrateurs)]** .

2 Sous l'onglet **[Folders (Dossiers)]** , sélectionnez le dossier et cliquez sur **[Remove Folder (Supprimer le dossier)]** .

3 Cliquez sur **[OK]** pour supprimer le dossier.

Consulter les pools de postes de travail dans un dossier

Vous pouvez voir tous les pools de postes de travail dans un dossier particulier dans View Administrator.

Procédure

1 Dans View Administrator, sélectionnez **[Inventory (Inventaire)] > [Pools]** .

La page Pools affiche les pools dans tous les dossiers par défaut.

2 Sélectionnez le dossier dans le menu déroulant **[Folder (Dossier)]** .

La page Pools affiche les pools dans le dossier que vous avez sélectionné.

Consulter les postes de travail dans un dossier

Vous pouvez voir tous les postes de travail dans un dossier particulier dans View Administrator. Un poste de travail hérite du dossier depuis son pool.

Procédure

1 Dans View Administrator, sélectionnez **[Inventory (Inventaire)] > [Desktops (Postes de travail)]** .

La page Desktops (Postes de travail) affiche les postes de travail dans tous les dossiers par défaut.

2 Sélectionnez le dossier dans le menu déroulant **[Folder (Dossier)]** .

La page Desktops (Postes de travail) affiche les pools dans le dossier que vous avez sélectionné.

Gérer des rôles personnalisés

Vous pouvez utiliser View Administrator pour ajouter, modifier et supprimer des rôles personnalisés.

- Ajouter un rôle personnalisé page 51

  Si les rôles d'administrateur prédéfinis ne répondent pas à vos besoins, vous pouvez combiner des privilèges spécifiques pour créer vos propres rôles dans View Administrator.

- Modifier les privilèges dans un rôle personnalisé page 51

  Vous pouvez modifier les privilèges dans un rôle personnalisé. Vous ne pouvez pas modifier les rôles d'administrateur prédéfinis.

- Supprimer un rôle personnalisé page 51

  Vous pouvez supprimer un rôle personnalisé s'il n'est pas inclus dans une autorisation. Vous ne pouvez pas supprimer les rôles d'administrateur prédéfinis.

Ajouter un rôle personnalisé

Si les rôles d'administrateur prédéfinis ne répondent pas à vos besoins, vous pouvez combiner des privilèges spécifiques pour créer vos propres rôles dans View Administrator.

Prérequis

Familiarisez-vous avec les privilèges d'administrateur que vous pouvez utiliser pour créer des rôles personnalisés. Reportez-vous à la section « Rôles et privilèges prédéfinis », page 52.

Procédure

1 Dans View Administrator, sélectionnez **[View Configuration (Configuration de View)] > [Administrators (Administrateurs)]** .

2 Sous l'onglet **[Roles (Rôles)]** , cliquez sur **[Add Role (Ajouter un rôle)]** .

3 Saisissez un nom et une description pour le nouveau rôle, sélectionnez un ou plusieurs privilèges et cliquez sur **[OK]** .

Le nouveau rôle apparaît dans le volet de gauche.

Modifier les privilèges dans un rôle personnalisé

Vous pouvez modifier les privilèges dans un rôle personnalisé. Vous ne pouvez pas modifier les rôles d'administrateur prédéfinis.

Prérequis

Familiarisez-vous avec les privilèges d'administrateur que vous pouvez utiliser pour créer des rôles personnalisés. Reportez-vous à la section « Rôles et privilèges prédéfinis », page 52.

Procédure

1 Dans View Administrator, sélectionnez **[View Configuration (Configuration de View)] > [Administrators (Administrateurs)]** .

2 Sous l'onglet **[Roles (Rôles)]** , sélectionnez le rôle.

3 Cliquez sur **[Privileges (Privilèges)]** pour afficher les privilèges dans le rôle, puis sur **[Edit (Modifier)]** .

4 Sélectionnez ou désélectionnez des privilèges.

5 Cliquez sur **[OK]** pour enregistrer vos modifications.

Supprimer un rôle personnalisé

Vous pouvez supprimer un rôle personnalisé s'il n'est pas inclus dans une autorisation. Vous ne pouvez pas supprimer les rôles d'administrateur prédéfinis.

Prérequis

Si le rôle est inclus dans une autorisation, supprimez l'autorisation. Reportez-vous à la section « Supprimer une autorisation », page 47.

Procédure

1 Dans View Administrator, sélectionnez **[View Configuration (Configuration de View)] > [Administrators (Administrateurs)]** .

2 Sous l'onglet **[Roles (Rôles)]** , sélectionnez le rôle et cliquez sur **[Remove Role (Supprimer un rôle)]** .

Le bouton **[Remove Role (Supprimer un rôle)]** n'est pas disponible pour les rôles prédéfinis ou pour les rôles personnalisés inclus dans une autorisation.

3 Cliquez sur **[OK]** pour supprimer le rôle.

Rôles et privilèges prédéfinis

View Administrator comporte des rôles prédéfinis que vous pouvez affecter à vos utilisateurs et groupes d'administrateurs. Vous pouvez également créer vos propres rôles d'administrateur en combinant des privilèges sélectionnés.

- Rôles d'administrateur prédéfinis page 52

  Les rôles d'administrateur prédéfinis combinent tous les privilèges individuels requis pour effectuer des tâches d'administration habituelles. Vous ne pouvez pas modifier les rôles prédéfinis.

- Privilèges généraux page 54

  Les privilèges généraux contrôlent les opérations système, telles que l'affichage et la modification des paramètres généraux. Les rôles ne contenant que des privilèges généraux ne peuvent pas être appliqués à des dossiers.

- Privilèges spécifiques de l'objet page 55

  Les privilèges spécifiques de l'objet contrôlent les opérations sur des types spécifiques d'objets d'inventaire. Les rôles contenant des privilèges spécifiques de l'objet peuvent être appliqués à des dossiers.

- Privilèges internes page 55

  Certains des rôles d'administrateur prédéfinis contiennent des privilèges internes. Vous ne pouvez pas sélectionner de privilèges internes lorsque vous créez des rôles personnalisés.

Rôles d'administrateur prédéfinis

Les rôles d'administrateur prédéfinis combinent tous les privilèges individuels requis pour effectuer des tâches d'administration habituelles. Vous ne pouvez pas modifier les rôles prédéfinis.

Tableau 2-6 décrit les rôles prédéfinis et indique si un rôle peut être appliqué à un dossier.

Tableau 2-6. Rôles prédéfinis dans View Administrator

Rôle	Actions réalisables par l'utilisateur	S'applique à un dossier
Administrators (Administrateurs)	Effectuer toutes les opérations d'administrateur, y compris la création d'utilisateurs et de groupes d'administrateurs supplémentaires. Les administrateurs avec le rôle Administrators (Administrateurs) sur le dossier racine sont des super administrateurs car ils ont un accès complet à tous les objets d'inventaire dans le système. Comme le rôle Administrators (Administrateurs) contient tous les privilèges, vous devez l'affecter à un ensemble limité d'utilisateurs. À l'origine, ce rôle est attribué aux membres du groupe Administrators (Administrateurs) local sur votre hôte de View Connection Server sur le dossier racine. IMPORTANT Un administrateur doit avoir le rôle Administrators (Administrateurs) sur le dossier racine pour effectuer les tâches suivantes : ■ Ajouter et supprimer des dossiers. ■ Gérer des applications ThinApp et des paramètres de configuration dans View Administrator. ■ Voir et modifier des instances de View Transfer Server et le référentiel de Transfer Server. ■ Utiliser les commandes `vdmadmin` et `vdmimport`.	Oui
Administrators (Read Only) (Administrateurs (lecture seule))	■ Voir, mais pas modifier, des paramètres généraux et des objets d'inventaire. ■ Voir, mais pas modifier, des applications ThinApp et des paramètres, des instances de View Transfer Server et le référentiel de Transfer Server. ■ Exécutez toutes les commandes PowerShell et les utilitaires de ligne de commande, en incluant `vdmexport` mais en excluant `vdmadmin` et `vdmimport`. Lorsque des administrateurs ont ce rôle sur un dossier, ils ne peuvent voir que les objets d'inventaire dans ce dossier.	Oui
Agent Registration Administrators (Administrateurs d'inscription d'agent)	Enregistrer des sources de postes de travail non gérées telles que des systèmes physiques, des machines virtuelles autonomes et des serveurs Terminal Server.	Non
Global Configuration and Policy Administrators (Administrateurs de configuration et règles générales)	Voir et modifier des règles générales et des paramètres de configuration sauf pour des rôles et autorisations d'administrateur, des applications ThinApp et des paramètres, des instances de View Transfer Server et le référentiel de Transfer Server.	Non
Global Configuration and Policy Administrators (Read only) (Administrateurs de configuration et règles générales (lecture seule))	Voir, mais pas modifier, des règles générales et des paramètres de configuration sauf pour des rôles et autorisations d'administrateur, des applications ThinApp et des paramètres, des instances de View Transfer Server et le référentiel de Transfer Server.	Non

Tableau 2-6. Rôles prédéfinis dans View Administrator (suite)

Rôle	Actions réalisables par l'utilisateur	S'applique à un dossier
Inventory Administrators (Administrateurs d'inventaire)	■ Effectuer toutes les opérations liées aux postes de travail, aux sessions et aux pools. ■ Gérer des disques persistants. ■ Resynchroniser, actualiser et rééquilibrer des pools de clone lié et modifier l'image de pool par défaut. Lorsque des administrateurs ont ce rôle sur un dossier, ils ne peuvent effectuer ces opérations que sur les objets d'inventaire dans ce dossier.	Oui
Inventory Administrators (Read only) (Administrateurs d'inventaire (lecture seule))	Voir, mais pas modifier, des objets d'inventaire. Lorsque des administrateurs ont ce rôle sur un dossier, ils ne peuvent voir que les objets d'inventaire dans ce dossier.	Oui

Privilèges généraux

Les privilèges généraux contrôlent les opérations système, telles que l'affichage et la modification des paramètres généraux. Les rôles ne contenant que des privilèges généraux ne peuvent pas être appliqués à des dossiers.

Tableau 2-7 décrit les privilèges généraux et répertorie les rôles prédéfinis qui contiennent chaque privilège.

Tableau 2-7. Privilèges généraux

Privilège	Actions réalisables par l'utilisateur	Rôles prédéfinis
Console Interaction (Interaction de console)	Ouvrir une session sur et utiliser View Administrator.	Administrators (Administrateurs) Administrators (Read Only) (Administrateurs (lecture seule)) Inventory Administrators (Administrateurs d'inventaire) Inventory Administrators (Read only) (Administrateurs d'inventaire (lecture seule)) Global Configuration and Policy Administrators (Administrateurs de configuration et règles générales) Global Configuration and Policy Administrators (Read only) (Administrateurs de configuration et règles générales (lecture seule))
Direct Interaction (Interaction directe)	Exécutez toutes les commandes PowerShell et les utilitaires de ligne de commande, sauf pour `vdmadmin` et `vdmimport`. Les administrateurs doivent avoir le rôle Administrators sur le dossier racine pour utiliser les commandes `vdmadmin` et `vdmimport`.	Administrators (Administrateurs) Administrators (Read Only) (Administrateurs (lecture seule))
Manage Global Configuration and Policies (Gérer la configuration et les règles générales)	Voir et modifier des règles générales et des paramètres de configuration sauf pour les rôles et les autorisations d'administrateur.	Administrators (Administrateurs) Global Configuration and Policy Administrators (Administrateurs de configuration et règles générales)

Tableau 2-7. Privilèges généraux (suite)

Privilège	Actions réalisables par l'utilisateur	Rôles prédéfinis
Manage Roles and Permissions (Gérer des rôles et autorisations)	Créer, modifier et supprimer des rôles et des autorisations d'administrateur.	Administrators (Administrateurs)
Register Agent (Inscrire l'agent)	Installer View Agent sur des sources de postes de travail non gérées, telles que des systèmes physiques, des machines virtuelles autonomes et des serveurs Terminal Server. Lors de l'installation de View Agent, vous devez fournir des informations d'identification administrateur pour inscrire la source de postes de travail non gérée avec l'instance de View Connection Server.	Administrators (Administrateurs) Agent Registration Administrators (Administrateurs d'inscription d'agent)

Privilèges spécifiques de l'objet

Les privilèges spécifiques de l'objet contrôlent les opérations sur des types spécifiques d'objets d'inventaire. Les rôles contenant des privilèges spécifiques de l'objet peuvent être appliqués à des dossiers.

Tableau 2-8 décrit les privilèges spécifiques de l'objet. Les rôles prédéfinis Administrators (Administrateurs) et Inventory Administrators (Administrateurs d'inventaire) contiennent tous les privilèges.

Tableau 2-8. Privilèges spécifiques de l'objet

Privilège	Actions réalisables par l'utilisateur	Objet
Enable Pool (Activer le pool)	Activer et désactiver des pools de postes de travail.	Pool de postes de travail
Entitle Pool (Autoriser un pool)	Ajouter et supprimer des autorisations d'utilisateur.	Pool de postes de travail
Manage Composer Pool Image (Gérer l'image de pool de Composer)	Resynchroniser, actualiser et rééquilibrer des pools de clone lié et modifier l'image de pool par défaut.	Pool de postes de travail
Manage Desktop (Gérer un poste de travail)	Effectuer toutes les opérations liées aux postes de travail et aux sessions.	Poste de travail
Manage Local Sessions (Gérer des sessions locales)	Restaurer et initier des réplications pour des postes de travail locaux.	Poste de travail
Manage Persistent Disks (Gérer des disques persistants)	Effectuer toutes les opérations de disque persistant de View Composer, y compris l'attachement, le détachement et l'importation des disques persistants.	Disque persistant
Manage Pool (Gérer un pool)	Ajouter, modifier et supprimer des pools de postes de travail et ajouter et supprimer des postes de travail.	Pool de postes de travail
Manage Remote Sessions (Gérer des sessions distantes)	Déconnecter et fermer des sessions distantes et envoyer des messages à des utilisateurs de poste de travail.	Poste de travail
Manage Reboot Operation (Gérer l'opération de redémarrage)	Réinitialiser des postes de travail.	Poste de travail

Privilèges internes

Certains des rôles d'administrateur prédéfinis contiennent des privilèges internes. Vous ne pouvez pas sélectionner de privilèges internes lorsque vous créez des rôles personnalisés.

Tableau 2-9 décrit les privilèges internes et répertorie les rôles prédéfinis qui contiennent chaque privilège.

Tableau 2-9. Privilèges internes

Privilège	Description	Rôles prédéfinis
Full (Read only) (Complet (lecture seule))	Accorde un accès en lecture seule à tous les paramètres.	Administrators (Read Only) (Administrateurs (lecture seule))
Manage Inventory (Read only) (Gérer l'inventaire (lecture seule))	Accorde un accès en lecture seule à des objets d'inventaire.	Inventory Administrators (Read only) (Administrateurs d'inventaire (lecture seule))
Manage Global Configuration and Policies (Read only) (Gérer la configuration et les règles générales (lecture seule))	Accorde un accès en lecture seule à des paramètres de configuration et des règles générales, sauf pour les administrateurs et les rôles.	Global Configuration and Policy Administrators (Read only) (Administrateurs de configuration et règles générales (lecture seule))

Privilèges requis pour des tâches habituelles

Beaucoup de tâches d'administration habituelles requièrent un jeu coordonné de privilèges. Certaines opérations requièrent une autorisation sur le dossier racine ainsi qu'un accès sur l'objet en cours de manipulation.

Privilèges pour la gestion des pools

Un administrateur doit posséder certains privilèges pour gérer des pools dans View Administrator.

Tableau 2-10 répertorie des tâches de gestion des pools communes et montre les privilèges requis pour effectuer chaque tâche. Vous effectuez ces tâches sur la page Pools dans View Administrator.

Tableau 2-10. Privilèges et tâches de gestion des pools

Tâche	Privilèges requis
Activer ou désactiver un pool	**Enable Pool (Activer le pool)** sur le pool.
Autoriser ou supprimer l'autorisation d'utilisateurs sur un pool	**Entitle Pool (Autoriser un pool)** sur le pool.
Ajouter un pool	**Manage Pool (Gérer un pool)** IMPORTANT Lors de l'ajout d'un pool de clone lié, vous devez posséder le rôle Administrators (Administrateurs) sur le dossier racine pour publier l'image de base sur le référentiel de Transfer Server.
Modifier ou supprimer un pool	**Manage Pool (Gérer un pool)** sur le pool.
Ajouter ou supprimer des postes de travail d'un pool	**Manage Pool (Gérer un pool)** sur le pool.
Actualiser, recomposer, rééquilibrer ou modifier l'image de View Composer par défaut	**Manage Composer Pool Image (Gérer l'image de pool de Composer)** sur le pool.
Modifier des dossiers	**[Manage Pool (Gérer un pool)]** sur les dossiers source et cible.

Privilèges pour la gestion des postes de travail

Un administrateur doit posséder certains privilèges pour gérer des postes de travail dans View Administrator.

Tableau 2-11 répertorie des tâches de gestion des postes de travail communes et montre les privilèges requis pour effectuer chaque tâche. Vous effectuez ces tâches sur la page Desktops (Postes de travail) dans View Administrator.

Tableau 2-11. Privilèges et tâches de gestion des postes de travail

Tâche	Privilèges requis
Supprimer une machine virtuelle	**Manage Pool (Gérer un pool)** sur le pool.
Réinitialiser une machine virtuelle	**Manage Reboot Operation (Gérer l'opération de redémarrage)** sur le poste de travail.
Annuler, interrompre ou reprendre une tâche	**Manage Composer Pool Image (Gérer l'image de pool de Composer)**
Affecter ou supprimer une propriété d'utilisateur	**Manage Desktop (Gérer un poste de travail)** sur le poste de travail.
Entrer ou quitter le mode de maintenance	**Manage Desktop (Gérer un poste de travail)** sur le poste de travail.
Restaurer ou initier des réplications	**Manage Local Sessions (Gérer des sessions locales)** sur le poste de travail.
Se déconnecter ou fermer une session distante	**Manage Remote Sessions (Gérer des sessions distantes)** sur le poste de travail.

Privilèges pour la gestion des disques persistants

Un administrateur doit posséder certains privilèges pour gérer des disques persistants dans View Administrator.

Tableau 2-12 répertorie des tâches de gestion des disques persistants communes et montre les privilèges requis pour effectuer chaque tâche. Vous effectuez ces tâches sur la page Persistent Disks (Disques persistants) dans View Administrator.

Tableau 2-12. Privilèges et tâches de gestion des disques persistants

Tâche	Privilèges requis
Détacher un disque	**Manage Persistent Disks (Gérer des disques persistants)** sur le disque et **Manage Pool (Gérer un pool)** sur le pool.
Attacher un disque	**Manage Persistent Disks (Gérer des disques persistants)** sur le disque et **Manage Pool (Gérer un pool)** sur le poste de travail.
Modifier un disque	**Manage Persistent Disks (Gérer des disques persistants)** sur le disque et **Manage Pool (Gérer un pool)** sur le pool sélectionné.
Modifier des dossiers	**Manage Persistent Disks (Gérer des disques persistants)** sur les dossiers source et cible.
Recréer un poste de travail	**Manage Persistent Disks (Gérer des disques persistants)** sur le disque et **Manage Pool (Gérer un pool)** sur le dernier pool.
Importer depuis vCenter	**Manage Persistent Disks (Gérer des disques persistants)** sur le dossier et **Manage Pool (Gérer un pool)** sur le pool.
Supprimer un disque	**Manage Persistent Disks (Gérer des disques persistants)** sur le disque.

Privilèges pour la gestion des utilisateurs et des administrateurs

Un administrateur doit posséder certains privilèges pour gérer des utilisateurs et des administrateurs dans View Administrator.

Tableau 2-13 répertorie des tâches de gestion des utilisateurs et des administrateurs communes et montre les privilèges requis pour effectuer chaque tâche. Vous gérez des utilisateurs sur la page Users and Groups (Utilisateurs et groupes) dans View Administrator. Vous gérez des administrateurs sur la page Global Administrators View (Vue générale des administrateurs) dans View Administrator.

Tableau 2-13. Privilèges et tâches de gestion des utilisateurs et des administrateurs

Tâche	Privilèges requis
Mettre à jour des informations utilisateur générales	**Manage Global Configuration and Policies (Gérer la configuration et les règles générales)**
Envoyer des messages à des utilisateurs de poste de travail	**Manage Remote Sessions (Gérer des sessions distantes)** sur le poste de travail.
Ajouter un utilisateur ou un groupe d'administrateurs	**Manage Roles and Permissions (Gérer des rôles et autorisations)**
Ajouter, modifier ou supprimer une autorisation d'administrateur	**Manage Roles and Permissions (Gérer des rôles et autorisations)**
Ajouter, modifier ou supprimer un rôle d'administrateur	**Manage Roles and Permissions (Gérer des rôles et autorisations)**

Privilèges pour des tâches et des commandes d'administration générales

Un administrateur doit posséder certains privilèges pour effectuer des tâches d'administration générales et exécuter des utilitaires de ligne de commande.

Tableau 2-14 montre les privilèges requis pour exécuter des tâches d'administration générale et exécuter des utilitaires de ligne de commande.

Tableau 2-14. Privilèges pour des tâches et des commandes d'administration générales

Tâche	Privilèges requis
Ajouter ou supprimer un dossier	Doit posséder le rôle Administrators (Administrateurs) sur le dossier racine.
Gérer des applications ThinApp et des paramètres dans View Administrator	Doit posséder le rôle Administrators (Administrateurs) sur le dossier racine.
Voir et modifier des instances de View Transfer Server et le référentiel de Transfer Server	Doit posséder le rôle Administrators (Administrateurs) sur le dossier racine.
Installer View Agent sur une source de postes de travail non gérée, telle qu'un système physique, une machine virtuelle autonome ou un serveur Terminal Server	**Register Agent (Inscrire l'agent)**
Voir ou modifier des paramètres de configuration (sauf pour les administrateurs) dans View Administrator	**Manage Global Configuration and Policies (Gérer la configuration et les règles générales)**
Exécutez toutes les commandes PowerShell et les utilitaires de ligne de commande, sauf pour `vdmadmin` et `vdmimport`.	**Direct Interaction (Interaction directe)**
Utiliser les commandes `vdmadmin` et `vdmimport`	Doit posséder le rôle Administrators (Administrateurs) sur le dossier racine.
Utiliser la commande `vdmexport`	Doit posséder le rôle Administrators (Administrateurs) ou le rôle Administrators (Read only) (Administrateurs (lecture seule)) sur le dossier racine.

Meilleures pratiques pour des utilisateurs et des groupes d'administrateurs

Pour augmenter la sécurité et la gérabilité de votre environnement View, vous devez suivre des meilleures pratiques lorsque vous gérez des utilisateurs et des groupes d'administrateurs.

- Comme le rôle Administrators contient tous les privilèges, affectez-le à un seul utilisateur ou à un ensemble limité d'utilisateurs.
- Choisissez un utilisateur ou un groupe Windows local pour avoir le rôle Administrators.
- Créez de nouveaux groupes d'utilisateurs pour les administrateurs. Évitez d'utiliser des groupes intégrés Windows ou d'autres groupes existants qui peuvent contenir des utilisateurs ou des groupes supplémentaires.
- Comme il est très visible et peut être facilement deviné, évitez d'utiliser le nom Administrator lorsque vous créez des utilisateurs et des groupes d'administrateurs.
- Créez des dossiers pour séparer les postes de travail sensibles. Déléguez l'administration de ces dossiers à un ensemble limité d'utilisateurs.
- Créez des administrateurs séparés qui peuvent modifier des règles générales et des paramètres de configuration View.

Préparation de sources de postes de travail non gérées 3

Les utilisateurs peuvent accéder à des postes de travail View fournis par des ordinateurs non gérés par vCenter Server. Ces sources de postes de travail non gérées peuvent inclure des ordinateurs physiques, des serveurs Terminal Server et des machines virtuelles exécutées sur VMware Server et d'autres plates-formes de virtualisation. Vous devez préparer une source de postes de travail non gérée pour fournir un accès au poste de travail View.

Ce chapitre aborde les rubriques suivantes :

Préparer une source de postes de travail non gérée pour un déploiement de poste de travail View

Vous devez effectuer certaines tâches pour préparer une source de postes de travail non gérée pour un déploiement de poste de travail View.

Prérequis

- Vérifiez que vous disposez de droits d'administration sur la source de postes de travail non gérée.
- Pour vous assurer que les utilisateurs de postes de travail View sont ajoutés au groupe Utilisateurs du Bureau à distance local de la source de postes de travail non gérée, créez un groupe Utilisateurs du Bureau à distance restreint dans Active Directory. Pour plus d'informations, consultez le document *Installation de VMware Horizon View*.

Procédure

1. Activez la source de postes de travail non gérée et vérifiez qu'elle est accessible à l'instance de Serveur de connexion View.
2. Associez la source de postes de travail non gérée au domaine Active Directory pour vos postes de travail View.
3. Configurez le pare-feu Windows pour autoriser des connexions Bureau à distance vers la source de postes de travail non gérée.

Suivant

Installez View Agent sur la source de postes de travail non gérée. Reportez-vous à la section « Installer View Agent sur une source de postes de travail non gérée », page 62.

Installer View Agent sur une source de postes de travail non gérée

Vous devez installer View Agent sur toutes les sources de postes de travail non gérées. View ne peut pas gérer une source de postes de travail non gérée sauf si View Agent est installé.

Pour installer View Agent sur plusieurs ordinateurs physiques Windows sans avoir à répondre à des invites d'assistant, vous pouvez installer View Agent en silence. Reportez-vous à la section « Installer View Agent en silence », page 73.

Prérequis

- Vérifiez que vous disposez de droits d'administration sur la source de postes de travail non gérée.
- Familiarisez-vous avec les options d'installation personnalisée de View Agent pour des sources de postes de travail non gérées. Reportez-vous à la section « Options d'installation personnalisée de View Agent pour des sources de postes de travail non gérées », page 63.
- Familiarisez-vous avec les ports TCP que le programme d'installation de View Agent ouvre sur le pare-feu. Pour plus d'informations, consultez le document *Planification de l'architecture de VMware Horizon View*.
- Téléchargez le fichier du programme d'installation View Agent sur la page du produit VMware sur http://www.vmware.com/fr/products/.

Procédure

1 Pour démarrer le programme d'installation de View Agent, double-cliquez sur le fichier du programme d'installation.

  Le nom de fichier du programme d'installation est `VMware-viewagent-y.y.y-xxxxxx.exe` ou `VMware-viewagent-x86_64-y.y.y-xxxxxx.exe`, où *y.y.y* est le numéro de version et *xxxxxx* le numéro de build.

2 Acceptez les termes de licence VMware.

3 Sélectionnez les options d'installation personnalisée désirées.

4 Acceptez ou modifiez le dossier de destination.

5 Dans la zone de texte **[Serveur]** , saisissez le nom d'hôte ou l'adresse IP d'un hôte de Serveur de connexion View.

  Lors de l'installation, le programme d'installation inscrit la source de postes de travail non gérée avec cette instance de Serveur de connexion View. Après l'inscription, l'instance de Serveur de connexion View spécifiée, et toutes les instances supplémentaires dans le même groupe Serveur de connexion View, peuvent communiquer avec la source de postes de travail non gérée.

6 Sélectionnez une méthode d'authentification pour inscrire la source de postes de travail non gérée avec l'instance de Serveur de connexion View.

Option	Action
S'authentifier comme étant l'utilisateur actuellement connecté	Les zones de texte **[Nom d'utilisateur]** et **[Mot de passe]** sont désactivées et vous ouvrez une session sur l'instance de Serveur de connexion View avec vos nom d'utilisateur et mot de passe actuels.
Spécifier les informations d'identification de l'administrateur	Vous devez fournir le nom d'utilisateur et le mot de passe d'un administrateur Serveur de connexion View dans les zones de texte **[Nom d'utilisateur]** et **[Mot de passe]** .

7 Suivez les invites dans le programme d'installation de View Agent et terminez l'installation.

8 Si vous avez sélectionné l'option de redirection USB, redémarrez la source de postes de travail non gérée pour activer la prise en charge USB.

De plus, l'assistant **[Nouveau matériel détecté]** doit démarrer. Suivez les invites dans l'assistant pour configurer le matériel avant de redémarrer la source de postes de travail non gérée.

Le service VMware View Agent est démarré sur la source de postes de travail non gérée.

Si Windows Media Player n'est pas installé, le programme d'installation de View Agent n'installe pas la fonction de redirection multimédia (MMR). Si vous installez Windows Media Player après l'installation de View Agent, vous pouvez installer la fonction MMR en exécutant de nouveau le programme d'installation de View Agent et en sélectionnant l'option Réparer.

Suivant

Utilisez la source de postes de travail non gérée pour créer un poste de travail View. Reportez-vous à la section « Pools de postes de travail manuels », page 136.

Options d'installation personnalisée de View Agent pour des sources de postes de travail non gérées

Lorsque vous installez View Agent sur une source de postes de travail non gérée, vous pouvez sélectionner certaines options d'installation personnalisée.

Tableau 3-1. Options d'installation personnalisée de View Agent pour des sources de postes de travail non gérées

Option	Description
Redirection USB	Donne aux utilisateurs un accès à des périphériques USB connectés en local sur leurs postes de travail. Windows 2003 et Windows 2008 ne prennent pas en charge la redirection USB. **Remarque** Vous pouvez utiliser les paramètres de stratégie de groupe pour désactiver une redirection USB pour des utilisateurs spécifiques.
PCoIP Server	Permet aux utilisateurs de se connecter au poste de travail View à l'aide du protocole d'affichage PCoIP. **Remarque** Sous Windows Vista, si vous installez le composant PCoIP Server, la stratégie de groupe Windows **[Disable or enable software Secure Attention Sequence (Désactiver ou activer la séquence de touches de sécurité (SAS, Secure Attention Sequence))]** est activée et définie sur **[Services]** et **[Ease of Access applications (Services et applications d'ergonomie)]** . Si vous modifiez ce paramètre, l'authentification unique ne fonctionne pas correctement.
PCoIP Smartcard	Permet aux utilisateurs de s'authentifier avec des cartes à puce lorsqu'ils utilisent le protocole d'affichage PCoIP.

Création et préparation de machines virtuelles

4

Vous pouvez utiliser des machines virtuelles gérées par vCenter Server pour approvisionner et déployer des postes de travail View. Vous pouvez utiliser une machine virtuelle gérée par vCenter Server en tant que modèle pour un pool automatisé, en tant que parent pour un pool de clone lié ou en tant que source de postes de travail dans un pool manuel. Vous devez préparer des machines virtuelles à fournir un accès au poste de travail View.

Ce chapitre aborde les rubriques suivantes :

Création de machines virtuelles pour un déploiement de poste de travail View

La machine virtuelle initiale établit un profil du matériel virtuel et du système d'exploitation à utiliser pour un déploiement rapide de postes de travail View.

1 Créer une machine virtuelle pour un déploiement de poste de travail View page 66

Vous utilisez vSphere Client pour créer des machines virtuelles dans vCenter Server pour des postes de travail View.

2 Installer un système d'exploitation client page 68

Après avoir créé une machine virtuelle, vous devez installer un système d'exploitation client.

3 Préparer un système d'exploitation client pour le déploiement de poste de travail View page 69

Vous devez effectuer certaines tâches pour préparer un système d'exploitation client pour le déploiement de poste de travail View.

Créer une machine virtuelle pour un déploiement de poste de travail View

Vous utilisez vSphere Client pour créer des machines virtuelles dans vCenter Server pour des postes de travail View.

Prérequis

- Téléchargez un fichier image ISO du système d'exploitation client vers un magasin de données sur votre serveur ESX.
- Familiarisez-vous avec les paramètres de configuration personnalisés pour les machines virtuelles. Reportez-vous à la section « Paramètres de configuration personnalisés de machine virtuelle », page 66.

Procédure

1. Dans vSphere Client, ouvrez une session sur le système vCenter Server.
2. Sélectionnez **[File (Fichier)] > [New (Nouveau)] > [Virtual Machine (Machine virtuelle)]** pour démarrer l'assistant New Virtual Machine (Nouvelle machine virtuelle).
3. Sélectionnez **[Custom (Personnaliser)]** et configurez des paramètres de configuration personnalisés.
4. Sélectionnez **[Edit the virtual machine settings before completion (Modifier les paramètres de la machine virtuelle avant l'achèvement)]** et cliquez sur **[Continue (Continuer)]** pour configurer des paramètres matériels.
   a. Ajoutez un lecteur CD/DVD, définissez le type de support pour utiliser un fichier image ISO, sélectionnez le fichier image ISO du système d'exploitation client que vous avez téléchargé vers votre magasin de données, puis sélectionnez **[Connect at power on (Se connecter à l'activation)]** .
   b. Si vous installez un système d'exploitation client Windows XP, ajoutez un lecteur de disquette et définissez le **[Device Type (Type de périphérique)]** sur **[Client Device (Périphérique client)]** .
   c. Définissez **[Power-on Boot Delay (Délai de démarrage d'activation)]** sur 10 000 millisecondes.
5. Cliquez sur **[Finish (Terminer)]** pour créer la machine virtuelle.

Suivant

Installez un système d'exploitation client sur la machine virtuelle.

Paramètres de configuration personnalisés de machine virtuelle

Vous pouvez utiliser des paramètres de configuration personnalisés de machine virtuelle comme paramètres de ligne de base lorsque vous créez une machine virtuelle pour le déploiement de poste de travail View.

Si vous utilisez View Administrator comme gestionnaire de poste de travail View pour déployer des postes de travail en pool, vous pouvez modifier ces paramètres lors du déploiement des postes de travail View basés sur des modèles.

Tableau 4-1. Paramètres de configuration personnalisés

Paramètre	Description et recommandations
Name and Location	Nom et emplacement de la machine virtuelle. Si vous prévoyez d'utiliser la machine virtuelle comme modèle, affectez un nom générique. L'emplacement peut être n'importe quel dossier de votre inventaire de datacenter.
Host/Cluster	Serveur ESX ou cluster de ressources de serveur qui exécutera la machine virtuelle. Si vous prévoyez d'utiliser la machine virtuelle comme modèle, l'emplacement de la machine virtuelle initiale ne spécifie pas nécessairement où résideront les futures machines virtuelles créées à partir du modèle.
Pool de ressources	Si les ressources de serveur ESX physiques sont divisées en pools de ressources, vous pouvez les affecter à la machine virtuelle.
Magasin de données	Emplacement de fichiers associés à la machine virtuelle.
Hardware Machine Version	Si vous créez la machine virtuelle sur un hôte ou un cluster ESXi 5.1 ou supérieur, vous pouvez sélectionner la version matérielle virtuelle 9 ou 8. La version 9 offre une meilleure fonctionnalité de la machine virtuelle. Si l'hôte ou le cluster est ESX/ESXi 5.0 ou supérieur, vous pouvez sélectionner la version matérielle virtuelle 8 ou 7. Si l'hôte ou le cluster est ESX/ESXi 4.0 ou supérieur, vous ne pouvez sélectionner que la version matérielle virtuelle 7.
Guest Operating System	Type de système d'exploitation que vous installerez sur la machine virtuelle.
CPUs	Nombre de processeurs virtuels dans la machine virtuelle. Pour la plupart des systèmes d'exploitation clients, un seul processeur est suffisant.
Mémoire	Quantité de mémoire à allouer à la machine virtuelle. Dans la plupart des cas, 512 Mo est suffisant.
Réseau	Nombre de cartes réseau dans la machine virtuelle. Une carte réseau est normalement suffisante. Le nom de réseau doit être cohérent dans les infrastructures virtuelles. Un nom de réseau incorrect dans un modèle peut provoquer des pannes lors des phases de personnalisation d'instance. Lorsque vous installez View Agent sur une machine virtuelle qui possède plusieurs cartes réseau, vous devez configurer le sous-réseau que View Agent utilise. Reportez-vous à la section « Configurer une machine virtuelle avec plusieurs cartes réseau pour View Agent », page 78 pour plus d'informations. **IMPORTANT** Pour les systèmes d'exploitation Windows 8, Windows 7 et Windows Vista, vous devez sélectionner l'adaptateur de réseau VMXNET 3. L'utilisation de l'adaptateur E1000 par défaut peut entraîner des erreurs d'expiration de personnalisation sur les machines virtuelles. Pour utiliser l'adaptateur VMXNET 3, vous devez installer un correctif Microsoft : ■ Pour Windows 7 SP1 : http://support.microsoft.com/kb/2550978 ■ Pour les versions Windows 7 antérieures à SP1 : http://support.microsoft.com/kb/2344941

Tableau 4-1. Paramètres de configuration personnalisés (suite)

Paramètre	Description et recommandations
`SCSI Controller`	Type d'adaptateur SCSI à utiliser avec la machine virtuelle. Pour les systèmes d'exploitation client Windows 8, Windows 7 et Windows XP, vous devez spécifier l'adaptateur LSI Logic. L'adaptateur LSI Logic a des performances améliorées et fonctionne mieux avec des périphériques SCSI génériques. LSI Logic SAS est disponible uniquement pour les machines virtuelles avec la version matérielle 7 et supérieure. **Remarque** Windows XP ne comporte pas de pilote pour l'adaptateur LSI Logic. Vous devez télécharger le pilote sur le site Web de LSI Logic.
`Select a Disk`	Disque à utiliser avec la machine virtuelle. Créez un nouveau disque virtuel basé sur la quantité de stockage local que vous décidez d'allouer à chaque utilisateur. Allouez assez d'espace de stockage pour l'installation du système d'exploitation, les correctifs et les applications installées en local. Pour réduire le besoin d'espace de disque et la gestion de données locales, vous devez stocker les informations, le profil et les documents de l'utilisateur sur des partages réseau plutôt que sur un disque local.

Installer un système d'exploitation client

Après avoir créé une machine virtuelle, vous devez installer un système d'exploitation client.

Prérequis

- Vérifiez qu'un fichier image ISO du système d'exploitation client se trouve sur un magasin de données sur votre serveur ESX.
- Vérifiez que le lecteur CD/DVD dans la machine virtuelle pointe vers le fichier image ISO du système d'exploitation client et que le lecteur CD/DVD est configuré pour se connecter lors de l'activation.
- Si vous installez Windows XP et que vous avez sélectionné l'adaptateur LSI Logic pour la machine virtuelle, téléchargez en aval le pilote du contrôleur LSI20320-R sur le site Web LSI Logic, créez un fichier image disquette (`.flp`) contenant le pilote et téléchargez en amont le fichier sur un magasin de données sur votre serveur ESX.

Procédure

1 Dans vSphere Client, ouvrez une session sur le système vCenter Server où réside la machine virtuelle.

2 Cliquez avec le bouton droit sur la machine virtuelle, sélectionnez **[Alimentation]**, puis **[Activer]** pour démarrer la machine virtuelle.

Comme vous avez configuré le lecteur CD/DVD pour qu'il pointe vers le fichier image ISO du système d'exploitation client et qu'il se connecte lors de l'activation, le processus d'installation du système d'exploitation client démarre automatiquement.

3 Cliquez sur l'onglet **[Console]** et suivez les instructions d'installation fournies par le fournisseur du système d'exploitation.

4 Si vous installez Windows XP et que vous avez sélectionné l'adaptateur LSI Logic pour la machine virtuelle, installez le pilote LSI Logic lors du processus d'installation de Windows.

a Appuyez sur F6 pour sélectionner des pilotes SCSI supplémentaires.

b Saisissez **S** pour spécifier un périphérique supplémentaire.

c Sur la barre d'outils vSphere Client, cliquez sur **[Connecter la disquette]** pour sélectionner le fichier image disquette (`.flp`) du pilote LSI Logic.

d Retournez à l'écran d'installation de Windows et appuyez sur Entrée pour continuer le processus d'installation de Windows.

e Quand le processus d'installation de Windows a terminé, déconnectez le lecteur de disquette virtuelle.

5 Si vous installez Windows 7 ou Windows 8, activez Windows en ligne.

Suivant

Préparez le système d'exploitation client pour le déploiement de poste de travail View.

Préparer un système d'exploitation client pour le déploiement de poste de travail View

Vous devez effectuer certaines tâches pour préparer un système d'exploitation client pour le déploiement de poste de travail View.

Prérequis

- Créez une machine virtuelle et installez un système d'exploitation client.
- Configurez un contrôleur de domaine Active Directory pour vos postes de travail View. Pour plus d'informations, consultez le document *Installation de VMware Horizon View*.
- Pour vous assurer que les utilisateurs de postes de travail View sont ajoutés au groupe Utilisateurs du Bureau à distance local de la machine virtuelle, créez un groupe Utilisateurs du Bureau à distance restreint dans Active Directory. Pour plus d'informations, consultez le document *Installation de VMware Horizon View*.
- Vérifiez que les services Bureau à distance, appelés Terminal Services sur les systèmes Windows XP, sont démarrés sur la machine virtuelle. Les services Bureau à distance sont requis pour l'installation de View Agent, l'authentification unique et d'autres opérations de View. Vous pouvez désactiver l'accès RDP vers vos postes de travail View en configurant des paramètres de pool de postes de travail et des paramètres de stratégie de groupe. Reportez-vous à la section « Empêcher l'accès à des postes de travail View via RDP », page 160.
- Vérifiez que vous disposez de droits d'administration sur le système d'exploitation client.
- Sur les systèmes d'exploitation Windows Vista, vérifiez que le service Windows Update est activé. Si vous désactivez ce service sous Windows Vista, le programme d'installation de View Agent ne parvient pas à installer le pilote USB.
- Si vous prévoyez de configurer le rendu graphique 3D pour des pools de postes de travail, familiarisez-vous avec le paramètre **[Activer la prise en charge 3D]** pour les machines virtuelles.

  Cette paramètre est actif sur les systèmes d'exploitation Windows 7 et supérieurs. Sur les hôtes ESXi 5.1 et supérieurs, vous pouvez également sélectionner des options qui déterminent comment le convertisseur 3D est géré sur l'hôte ESXi. Pour plus d'informations, consultez le document *Administration d'une machine virtuelle vSphere*.

Procédure

1 Dans vSphere Client, ouvrez une session sur le système vCenter Server où réside la machine virtuelle.

2 Cliquez avec le bouton droit sur la machine virtuelle, sélectionnez **[Alimentation]**, puis **[Activer]** pour démarrer la machine virtuelle.

3 Cliquez avec le bouton droit sur la machine virtuelle, sélectionnez **[Client]**, puis **[Installer/Mettre à niveau VMware Tools]** pour installer la dernière version de VMware Tools.

4 Utilisez la fonction de synchronisation de l'heure de VMware Tools pour vous assurer que la machine virtuelle est synchronisée avec ESX.

   ESX doit synchroniser avec une source NTP externe, par exemple, la même source d'heure qu'Active Directory.

   Désactivez les autres mécanismes de synchronisation de l'heure, tels que Service de temps Windows.

   L'aide en ligne de VMware Tools fournit des informations sur la configuration de la synchronisation de l'heure entre client et hôte.

5 Installez les packs de service et les mises à jour.

6 Installez un logiciel antivirus.

7 Installez d'autres applications et logiciels, tels que Windows Media Player si vous utilisez MMR et des pilotes de cartes à puce si vous utilisez l'authentification par carte à puce.

   Si vous prévoyez d'utiliser Horizon Workspace pour offrir un catalogue qui inclut des applications ThinApp, vous devez installer Horizon Agent.

   Sur les systèmes Windows XP, installez tous les logiciels et applications tiers (sauf Microsoft .NET Framework) avant d'installer View Agent.

   IMPORTANT Si vous installez Microsoft .NET Framework, vous devez l'installer après View Agent.

8 Si des clients View se connectent à la machine virtuelle avec le protocole d'affichage PCoIP, définissez l'option d'alimentation **[Éteindre l'écran]** sur **[Jamais]** .

   Si vous ne désactivez pas ce paramètre, l'écran semblera se figer dans son dernier état lorsque le mode d'économie d'énergie démarrera.

9 Si des clients View se connectent à la machine virtuelle avec le protocole d'affichage PCoIP, allez dans **[Panneau de configuration] > [Système] > [Paramètres système avancés] > [Paramètres de performances]** et, pour **[Effets visuels]** , choisissez le paramètre **[Ajuster afin d'obtenir les meilleures performances]** .

   Si vous utilisez plutôt le paramètre **[Ajuster afin d'obtenir la meilleure apparence]** ou **[Laisser Windows choisir la meilleure configuration]** et si Windows choisit l'apparence au lieu de la performance, la performance est affectée négativement.

10 Si un serveur proxy est utilisé dans votre environnement de réseau, configurez les paramètres du proxy réseau.

11 Configurez des propriétés de connexion réseau.

   a Affectez une adresse IP statique ou spécifiez qu'une adresse IP est affectée par un serveur DHCP.

      View ne prend pas en charge les adresses locales du lien (169.254.x.x) pour les postes de travail View.

   b Définissez les adresses de serveurs DNS préférentiels et alternatifs sur votre adresse de serveur Active Directory.

12 Associez la machine virtuelle au domaine Active Directory pour vos postes de travail View.

   Une machine virtuelle parente que vous utilisez pour View Composer doit appartenir au même domaine Active Directory que le domaine que les postes de travail de clone lié rejoindront ou doit être un membre du Groupe de travail local.

13 Configurez le pare-feu Windows pour autoriser des connexions Bureau à distance vers la machine virtuelle.

14 (Facultatif) Désactivez les périphériques PCI enfichables à chaud.

   Cette étape évite aux utilisateurs de déconnecter accidentellement le périphérique de réseau virtuel (vNIC) de la machine virtuelle.

15 (Facultatif) Configurez des scripts de personnalisation d'utilisateur.

Suivant

Installez View Agent. Reportez-vous à la section « Installer View Agent sur une machine virtuelle », page 71.

Installer View Agent sur une machine virtuelle

Vous devez installer View Agent sur des machines virtuelles gérées par vCenter Server pour que Serveur de connexion View puisse communiquer avec elles. Installez View Agent sur toutes les machines virtuelles que vous utilisez en tant que modèles pour les pools de postes de travail automatisés, en tant que parents pour les pools de postes de travail de clone lié et en tant que sources de postes de travail dans des pools de postes de travail manuels.

Pour installer View Agent sur plusieurs machines virtuelles Windows sans avoir à répondre à des invites d'assistant, vous pouvez installer View Agent en silence. Reportez-vous à la section « Installer View Agent en silence », page 73.

Le logiciel View Agent ne peut pas coexister sur la même machine virtuelle ou physique avec d'autres composants logiciels de View Manager, y compris un serveur de sécurité, un serveur réplica, Serveur de connexion View, View Composer, View Client ou Serveur de transfert View.

Prérequis

- Préparez le système d'exploitation client pour le déploiement de poste de travail View. Reportez-vous à la section « Préparer un système d'exploitation client pour le déploiement de poste de travail View », page 69.
- Téléchargez le fichier du programme d'installation View Agent sur la page du produit VMware sur http://www.vmware.com/fr/products/.
- Vérifiez que vous disposez de droits d'administration sur la machine virtuelle.
- Familiarisez-vous avec les options d'installation personnalisée de View Agent. Reportez-vous à la section « Options d'installation personnalisée de View Agent », page 72.
- Familiarisez-vous avec les ports TCP que le programme d'installation de View Agent ouvre sur le pare-feu. Pour plus d'informations, consultez le document *Planification de l'architecture de VMware Horizon View*.
- Si vous sélectionnez l'option d'installation personnalisée de View Composer Agent, vérifiez que vous possédez une licence pour utiliser View Composer.

Procédure

1 Pour démarrer le programme d'installation de View Agent, double-cliquez sur le fichier du programme d'installation.

Le nom de fichier du programme d'installation est `VMware-viewagent-y.y.y-xxxxxx.exe` ou `VMware-viewagent-x86_64-y.y.y-xxxxxx.exe`, où *y.y.y* est le numéro de version et *xxxxxx* le numéro de build.

2 Acceptez les termes de licence VMware.

3 Sélectionnez les options d'installation personnalisée désirées.

Pour déployer des postes de travail de clone lié, sélectionnez l'option **[View Composer Agent]** .

4 Acceptez ou modifiez le dossier de destination.

5 Suivez les invites dans le programme d'installation de View Agent et terminez l'installation.

Remarque Si vous n'avez pas activé la prise en charge du Bureau à distance au cours de la préparation du système d'exploitation client, le programme d'installation de View Agent vous invite à l'activer. Si vous n'activez pas la prise en charge du Bureau à distance au cours de l'installation de View Agent, vous devez l'activer manuellement une fois l'installation terminée.

6 Si vous avez sélectionné l'option de redirection USB, redémarrez la machine virtuelle pour activer la prise en charge USB.

De plus, l'assistant **[Nouveau matériel détecté]** doit démarrer. Suivez les invites dans l'assistant pour configurer le matériel avant de redémarrer la machine virtuelle.

Le service VMware View Agent est démarré sur la machine virtuelle.

Si vous avez sélectionné l'option **[View Composer Agent]** , le service VMware View Composer Guest Agent Server est démarré sur la machine virtuelle.

Si Windows Media Player n'est pas installé, le programme d'installation de View Agent n'installe pas la fonction de redirection multimédia (MMR). Si vous installez Windows Media Player après l'installation de View Agent, vous pouvez installer la fonction MMR en exécutant de nouveau le programme d'installation de View Agent et en sélectionnant l'option Réparer.

Suivant

Si la machine virtuelle contient plusieurs cartes réseau, configurez le sous-réseau que View Agent utilise. Reportez-vous à la section « Configurer une machine virtuelle avec plusieurs cartes réseau pour View Agent », page 78.

Options d'installation personnalisée de View Agent

Lorsque vous installez View Agent sur une machine virtuelle, vous pouvez sélectionner des options d'installation personnalisée.

Tableau 4-2. Options d'installation personnalisée de View Agent

Option	Description
Redirection USB	Donne aux utilisateurs un accès à des périphériques USB connectés en local sur leurs postes de travail. Windows 2003 et Windows 2008 ne prennent pas en charge la redirection USB. **Remarque** Vous pouvez utiliser les paramètres de stratégie de groupe pour désactiver une redirection USB pour des utilisateurs spécifiques.
View Composer Agent	Permet à View Agent de s'exécuter sur les postes de travail de clone lié déployés depuis cette machine virtuelle.
Impression virtuelle	Permet aux utilisateurs d'imprimer depuis n'importe quelle imprimante disponible sur leurs ordinateurs client Windows. Les utilisateurs n'ont pas à installer des pilotes supplémentaires sur leurs postes de travail.

Tableau 4-2. Options d'installation personnalisée de View Agent (suite)

Option	Description
Serveur PCoIP	Permet aux utilisateurs de se connecter au poste de travail View à l'aide du protocole d'affichage PCoIP. L'installation de la fonction PCoIP Server désactive le mode veille sur les postes de travail Windows 8, Windows 7, Windows Vista et Windows XP. Lorsqu'un utilisateur va dans le menu Options d'alimentation ou Arrêter, le mode veille est inactif. Les postes de travail ne passent pas en mode veille après une période par défaut d'inactivité. Les postes de travail restent en mode actif. **Remarque** Sous Windows Vista, si vous installez la fonction PCoIP Server, la stratégie de groupe Windows **[Désactiver ou activer la séquence de touches de sécurité (SAS, Secure Attention Sequence)]** est activée et définie sur **[Services]** et **[Services et applications d'ergonomie]** . Si vous modifiez ce paramètre, l'authentification unique ne fonctionne pas correctement.
Carte à puce PCoIP	Permet aux utilisateurs de s'authentifier avec des cartes à puce lorsqu'ils utilisent le protocole d'affichage PCoIP.
View Persona Management	Synchronise le profil d'utilisateur sur le poste de travail local avec un référentiel de profils distant, pour que les utilisateurs puissent accéder à leurs profils dès qu'ils ouvrent une session sur un poste de travail.

Installer View Agent en silence

Vous pouvez utiliser la fonction d'installation silencieuse de MSI (Microsoft Windows Installer) pour installer View Agent sur plusieurs machines virtuelles ou ordinateurs physiques Windows. Dans une installation silencieuse, vous utilisez la ligne de commande et n'avez pas à répondre à des invites d'assistant.

Avec l'installation silencieuse, vous pouvez déployer efficacement des composants View dans une grande entreprise.

Prérequis

- Préparez le système d'exploitation client pour le déploiement de poste de travail View. Reportez-vous à la section « Préparer un système d'exploitation client pour le déploiement de poste de travail View », page 69.
- Téléchargez le fichier du programme d'installation View Agent sur la page du produit VMware sur http://www.vmware.com/fr/products/.

  Le nom de fichier du programme d'installation est `VMware-viewagent-y.y.y-xxxxxx.exe` ou `VMware-viewagent-x86_64-y.y.y-xxxxxx.exe`, où *y.y.y* est le numéro de version et *xxxxxx* le numéro de build.
- Vérifiez que vous disposez de droits d'administration sur la machine virtuelle ou l'ordinateur physique.
- Familiarisez-vous avec les options d'installation personnalisée de View Agent. Reportez-vous à la section « Options d'installation personnalisée de View Agent », page 72.
- Si vous sélectionnez l'option d'installation personnalisée de View Composer Agent, vérifiez que vous possédez une licence pour utiliser View Composer.
- Familiarisez-vous avec les options de ligne de commande du programme d'installation MSI. Reportez-vous à la section « Options de ligne de commande Microsoft Windows Installer », page 74.
- Familiarisez-vous avec les propriétés d'installation silencieuse disponibles avec View Agent. Reportez-vous à la section « Propriétés de l'installation silencieuse pour View Agent », page 76.

- Familiarisez-vous avec les ports TCP que le programme d'installation de View Agent ouvre sur le pare-feu. Pour plus d'informations, consultez le document *Planification de l'architecture de VMware Horizon View*.

Procédure

1 Ouvrez une invite de commande Windows sur la machine virtuelle ou l'ordinateur physique.

2 Saisissez la commande d'installation sur une ligne.

Cet exemple installe View Agent dans une machine virtuelle gérée par vCenter Server. Le programme d'installation configure les options d'installation personnalisée : PCoIP, View Composer Agent, impression virtuelle et redirection USB.

```
VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn VDM_VC_MANAGED_AGENT=1
ADDLOCAL=Core,PCoIP,SVIAgent,ThinPrint,USB"
```

Cet exemple installe View Agent sur un ordinateur non géré et inscrit le poste de travail avec le serveur Serveur de connexion View spécifié, `cs1.companydomain.com`. Le programme d'installation configure les options d'installation personnalisée : authentification unique, impression virtuelle et redirection USB.

```
VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn VDM_VC_MANAGED_AGENT=0
VDM_SERVER_NAME=cs1.companydomain.com VDM_SERVER_USERNAME=admin.companydomain.com
VDM_SERVER_PASSWORD=secret ADDLOCAL=Core,ThinPrint,USB"
```

Le service VMware View Agent est démarré sur la machine virtuelle.

Si vous avez sélectionné l'option **[View Composer Agent]** , le service VMware View Composer Guest Agent Server est démarré sur la machine virtuelle.

Si Windows Media Player n'est pas installé, le programme d'installation de View Agent n'installe pas la fonction de redirection multimédia (MMR). Si vous installez Windows Media Player après l'installation de View Agent, vous pouvez installer la fonction MMR en exécutant de nouveau le programme d'installation de View Agent et en sélectionnant l'option Réparer.

Suivant

Si la machine virtuelle contient plusieurs cartes réseau, configurez le sous-réseau que View Agent utilise. Reportez-vous à la section « Configurer une machine virtuelle avec plusieurs cartes réseau pour View Agent », page 78.

Options de ligne de commande Microsoft Windows Installer

Pour installer des composants View en silence, vous devez utiliser des options et des propriétés de ligne de commande de MSI (Microsoft Windows Installer). Les programmes d'installation des composants View sont des programmes MSI et utilisent des fonctions MSI standard.

Pour plus d'informations sur MSI, consultez le site Web Microsoft. Pour connaître les options de ligne de commande MSI, consultez le site Web MSDN Library et recherchez des options de ligne de commande MSI. Pour voir comment utiliser la ligne de commande MSI, vous pouvez ouvrir une invite de commande sur l'ordinateur de composant View et saisir `msiexec /?`.

Pour exécuter un programme d'installation de composant View en silence, commencez par désactiver le programme de démarrage qui extrait le programme d'installation dans un répertoire temporaire et démarre une installation interactive.

Sur la ligne de commande, vous devez saisir les options de ligne de commande qui contrôlent le programme de démarrage du programme d'installation.

Tableau 4-3. Options de ligne de commande du programme de démarrage d'un composant View

Option	Description
`/s`	Désactive l'écran de démarrage et la boîte de dialogue d'extraction, qui empêche l'affichage de boîtes de dialogue interactives. Par exemple : `VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s` L'option `/s` est requise pour exécuter une installation silencieuse.
`/v" MSI_command_line_options"`	Demande au programme d'installation de transmettre la chaîne comprise entre guillemets doubles que vous saisissez sur la ligne de commande sous forme de jeu d'options que MSI doit interpréter. Vous devez insérer des guillemets doubles avant et après vos entrées de ligne de commande. Placez un guillemet double après `/v` et à la fin de la ligne de commande. Par exemple : `VMware-viewagent-y.y.y-xxxxxx.exe /s /v"command_line_options"` Pour demander au programme d'installation MSI d'interpréter une chaîne contenant des espaces, insérez deux jeux de guillemets doubles avant et après la chaîne. Pour exemple, vous voulez peut-être installer le composant View dans un nom de chemin d'installation contenant des espaces. Par exemple : `VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"command_line_options INSTALLDIR=""d:\abc\my folder"""` Dans cet exemple, le programme d'installation MSI transmet le chemin du répertoire d'installation et n'essaie pas d'interpréter la chaîne comme deux options de ligne de commande. Notez le guillemet double final entourant toute la ligne de commande. L'option `/v"command_line_options"` est requise pour exécuter une installation silencieuse.

Vous contrôlez le reste de l'installation silencieuse en transmettant des options de ligne de commande et des valeurs de propriété MSI au programme d'installation MSI, `msiexec.exe`. Le programme d'installation MSI comporte le code d'installation du composant View. Le programme d'installation utilise les valeurs et les options que vous saisissez dans la ligne de commande pour interpréter des choix d'installation et des options de configuration spécifiques au composant View.

Tableau 4-4. Options de ligne de commande MSI et propriétés MSI

Option ou propriété MSI	Description
`/qn`	Demande au programme d'installation MSI de ne pas afficher les pages de l'assistant d'installation. Par exemple, vous voulez peut-être installer View Agent en silence et n'utiliser que des options et des fonctions d'installation par défaut : `VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn"` Vous pouvez également utiliser l'option `/qb` pour afficher les pages de l'assistant dans une installation non interactive et automatisée. Lors de l'installation, les pages de l'assistant sont affichées, mais vous ne pouvez pas y répondre. L'option `/qn` ou `/qb` est requise pour exécuter une installation silencieuse.
`INSTALLDIR`	Spécifie un autre chemin d'installation pour le composant View. Utilisez le format *INSTALLDIR=path* pour spécifier un chemin d'installation. Vous pouvez ignorer cette propriété MSI si vous voulez installer le composant View dans le chemin par défaut. Cette propriété MSI est facultative.

Tableau 4-4. Options de ligne de commande MSI et propriétés MSI (suite)

Option ou propriété MSI	Description
ADDLOCAL	Détermine les fonctions spécifiques du composant à installer. Dans une installation interactive, le programme d'installation View affiche des options d'installation personnalisée à sélectionner. La propriété MSI, ADDLOCAL, vous permet de spécifier ces options d'installation sur la ligne de commande. Pour installer toutes les options d'installation personnalisée disponibles, saisissez ADDLOCAL=ALL. Par exemple : VMware-viewagent-*y.y.y-xxxxxx*.exe /s /v"/qn ADDLOCAL=ALL" Si vous n'utilisez pas la propriété MSI, ADDLOCAL, les options d'installation par défaut sont installées. Pour spécifier des options d'installation individuelles, saisissez une liste séparée par des virgules de noms d'option d'installation. N'utilisez pas d'espaces entre les noms. Utilisez le format *ADDLOCAL=value,value,value...*. Par exemple, vous voulez peut-être installer View Agent dans un système d'exploitation client avec les fonctions View Composer Agent et PCoIP : VMware-viewagent-*y.y.y-xxxxxx*.exe /s /v"/qn ADDLOCAL=Core,SVIAgent,PCoIP" **Remarque** La fonction Core est requise dans View Agent. Cette propriété MSI est facultative.
REBOOT	Vous pouvez utiliser l'option REBOOT=ReallySuppress pour permettre à des tâches de configuration système de s'exécuter avant le redémarrage du système. Cette propriété MSI est facultative.
/l*v *log_file*	Inscrit des informations de journalisation dans le fichier journal spécifié avec une sortie détaillée. Par exemple : /l*v ""%TEMP%\vmmsi.log"" Cet exemple génère un fichier journal détaillé semblable au journal généré lors d'une installation interactive. Vous pouvez utiliser cette option pour enregistrer des fonctions personnalisées qui peuvent s'appliquer de façon unique à votre installation. Vous pouvez utiliser les informations enregistrées pour spécifier des fonctions d'installation dans les installations silencieuses futures. L'option /l*v est facultative.

Propriétés de l'installation silencieuse pour View Agent

Vous pouvez inclure des propriétés spécifiques lorsque vous installez View Agent silencieusement depuis la ligne de commande. Vous devez utiliser un format *PROPERTY=value* pour que Microsoft Windows Installer (MSI) puisse interpréter les propriétés et les valeurs.

Tableau 4-5 montre les propriétés de l'installation silencieuse de View Agent que vous pouvez utiliser sur la ligne de commande.

Tableau 4-5. Propriétés MSI pour l'installation silencieuse de View Agent

Propriété MSI	Description	Valeur par défaut
INSTALLDIR	Chemin d'accès et dossier dans lequel le logiciel View Agent est installé. Par exemple : INSTALLDIR=""D:\abc\my folder"" Les jeux de deux guillemets doubles entourant le chemin autorisent le programme d'installation MSI à ignorer l'espace dans le chemin. Cette propriété MSI est facultative.	%ProgramFiles%\VMware\VMware View\Agent
RDPCHOICE	Détermine l'activation du protocole RDP (Remote Desktop Protocol) sur le poste de travail. Une valeur de 1 active RDP. Une valeur de 0 laisse le paramètre RDP désactivé. Cette propriété MSI est facultative.	1

Tableau 4-5. Propriétés MSI pour l'installation silencieuse de View Agent (suite)

Propriété MSI	Description	Valeur par défaut
VDM_VC_MANAGED_AGENT	Détermine si vCenter Server gère la machine virtuelle sur laquelle View Agent est installé. Une valeur de 1 configure le poste de travail en tant que machine virtuelle gérée par vCenter Server. Une valeur de 0 configure le poste de travail comme étant non géré par vCenter Server. Cette propriété MSI est requise.	Aucune
VDM_SERVER_NAME	Nom d'hôte ou adresse IP de l'ordinateur Serveur de connexion View sur lequel le programme d'installation de View Agent inscrit un poste de travail non géré. Cette propriété s'applique uniquement à des postes de travail non gérés. Par exemple : VDM_SERVER_NAME=10.123.01.01 Cette propriété MSI est requise pour les postes de travail non gérés. N'utilisez pas cette propriété MSI pour les postes de travail de machine virtuelle gérés par vCenter Server.	Aucune
VDM_SERVER_USERNAME	Nom d'utilisateur de l'administrateur sur l'ordinateur Serveur de connexion View. Cette propriété MSI s'applique uniquement à des postes de travail non gérés. Par exemple : VDM_SERVER_USERNAME=admin.companydomain.com Cette propriété MSI est requise pour les postes de travail non gérés. N'utilisez pas cette propriété MSI pour les postes de travail de machine virtuelle gérés par vCenter Server.	Aucune
VDM_SERVER_PASSWORD	Mot de passe d'utilisateur administrateur de Serveur de connexion View. Par exemple : VDM_SERVER_PASSWORD=secret Cette propriété MSI est requise pour les postes de travail non gérés. N'utilisez pas cette propriété MSI pour les postes de travail de machine virtuelle gérés par vCenter Server.	Aucune

Dans une commande d'installation silencieuse, vous pouvez utiliser la propriété MSI, ADDLOCAL=, pour spécifier des fonctions personnalisées que le programme d'installation de View Agent configure. Chaque fonction d'installation silencieuse correspond à une option d'installation personnalisée que vous pouvez sélectionner au cours d'une installation interactive.

Tableau 4-6 montre les fonctions View Agent que vous pouvez saisir sur la ligne de commande et les options d'installation personnalisée correspondantes.

Tableau 4-6. Fonctions d'installation silencieuse de View Agent et options d'installation personnalisée interactive

Fonction d'installation silencieuse	Option d'installation personnalisée dans une installation interactive
Core. Si vous spécifiez des fonctions individuelles avec la propriété MSI, ADDLOCAL=, vous devez inclure Core. Si vous spécifiez ADDLOCAL=ALL, toutes les fonctions, y compris Core, sont installées.	Aucune. Au cours d'une installation interactive, les fonctions principales de View Agent sont installées par défaut.
SVIAgent	View Composer Agent
ThinPrint	Impression virtuelle
ThinPrintPCoIP	Impression virtuelle avec PCoIP
PCoIP	Protocole PCoIP
USB	Redirection USB

Tableau 4-6. Fonctions d'installation silencieuse de View Agent et options d'installation personnalisée interactive (suite)

Fonction d'installation silencieuse	Option d'installation personnalisée dans une installation interactive
VPA	View Persona Management (Gestion de persona View)
VmVideo	Dans une installation interactive, cette fonction n'est pas une option d'installation personnalisée séparée.
VmwVAudio	Dans une installation interactive, cette fonction n'est pas une option d'installation personnalisée séparée.
SmartCard	Dans une installation interactive, la fonction SmartCard n'est pas une option d'installation personnalisée séparée.
VMCI	Dans une installation interactive, la fonction VMCI n'est pas une option d'installation personnalisée séparée.

Pour plus d'informations sur les options d'installation personnalisée, reportez-vous à la section « Options d'installation personnalisée de View Agent », page 72.

Configurer une machine virtuelle avec plusieurs cartes réseau pour View Agent

Lorsque vous installez View Agent sur une machine virtuelle qui possède plusieurs cartes réseau, vous devez configurer le sous-réseau que View Agent utilise. Le sous-réseau détermine quelle adresse réseau est fournie par View Agent à l'instance de View Connection Server pour les connexions de protocole client.

Procédure

- Sur la machine virtuelle sur laquelle View Agent est installée, ouvrez une invite de commande, saisissez **`regedit.exe`** et créez une entrée de registre pour configurer le sous-réseau.

  Par exemple : **`HKLM\Software\VMware, Inc.\VMware VDM\Node Manager\subnet = n.n.n.n/m (REG_SZ)`**

  Dans cet exemple, *n.n.n.n* est le sous-réseau TCP/IP et *m* est le nombre de bits dans le masque de sous-réseau.

Optimiser les performances du système d'exploitation Windows client

Vous pouvez suivre certaines étapes pour optimiser un système d'exploitation client pour le déploiement de poste de travail View. Ces étapes s'appliquent à tous les systèmes d'exploitation Windows. Toutes ces étapes sont facultatives.

Ces recommandations incluent la désactivation de l'écran de veille et la non spécification d'un temporisateur de veille. Votre entreprise peut requérir l'utilisation d'écrans de veille. Par exemple, vous pouvez avoir une règle de sécurité gérée par GPO qui verrouille un poste de travail un certain temps après le démarrage de l'écran de veille. Dans ce cas, utilisez un écran noir.

Prérequis

Préparez un système d'exploitation client pour le déploiement de poste de travail View.

Procédure

- Désactivez tous les ports inutiles, tels que COM1, COM2 et LPT.
- Modifiez les propriétés d'affichage.
  a Sélectionnez un thème de base.
  b Choisissez une couleur d'arrière-plan unie.

c Réglez l'écran de veille sur **[Aucun]** .

d Vérifiez que l'accélération matérielle est activée.

- Sélectionnez une option d'alimentation haute performance sans spécifier de temporisateur de veille.
- Désactivez le composant Service d'indexation.

REMARQUE L'indexation améliore les recherches en cataloguant les fichiers. Ne désactivez pas cette fonction pour les utilisateurs qui effectuent souvent des recherches.

- Supprimez ou réduisez les point de restauration du système.
- Désactivez la protection du système sur `C:\`.
- Désactivez tout service inutile.
- Réglez le son sur **[Aucun son]** .
- Réglez les effets visuels sur **[Ajuster pour de meilleures performances]** .
- Ouvrez Windows Media Player et utilisez les paramètres par défaut.
- Désactivez la maintenance automatique de l'ordinateur.
- Ajustez les paramètres de performance pour de meilleures performances.
- Supprimez tous les dossiers de désinstallation masqués dans `C:\Windows`, tels que `$NtUninstallKB893756$`.
- Supprimez tous les journaux d'événements.
- Exécutez un nettoyage du disque pour supprimer les fichiers temporaires, vider la Corbeille et éliminer les fichiers système et les autres éléments devenus inutiles.
- Exécutez Défragmenteur de disque pour réorganiser les données fragmentées.
- Si les utilisateurs veulent lire des vidéos en plein écran ou exécuter des applications 3D sur des postes de travail exécutés dans un environnement vSphere 5.1, suivez les instructions pour modifier le registre dans l'article 235257 de la Base de connaissances Microsoft.

  Cet article est intitulé « Le serveur n'utilise pas toute la bande passante disponible lors de la diffusion en continu de fichiers avec des vitesses de transmission supérieures à 100 Kbit/s » et se trouve à l'adresse http://support.microsoft.com/kb/235257. Redémarrez la machine virtuelle pour que le paramètre de registre modifié prenne effet.

  Sans cette optimisation, les images peuvent se figer brièvement ou les vidéos peuvent être saccadées.

  REMARQUE Cette optimisation permet d'améliorer les performances dans ESXi 5.x et ESXi 5.1, mais elle est requise pour ESXi 5.1.

Suivant

Pour les systèmes d'exploitation client Windows 7 et Windows 8, effectuez des tâches d'optimisation complémentaires. Reportez-vous à la section « Optimiser les performances du système d'exploitation client Windows 7 et Windows 8 », page 80.

Optimiser les performances du système d'exploitation client Windows 7 et Windows 8

Vous pouvez réaliser des étapes supplémentaires pour optimiser un système d'exploitation client Windows 7 et Windows 8 pour le déploiement de poste de travail View. Toutes ces étapes sont facultatives.

Prérequis

- Effectuez les opérations d'optimisation du système d'exploitation client qui s'appliquent à tous les systèmes d'exploitation Windows. Reportez-vous à la section « Optimiser les performances du système d'exploitation Windows client », page 78.
- Familiarisez-vous avec la procédure de désactivation du programme d'amélioration de l'expérience utilisateur Windows. Reportez-vous à la section « Désactiver le programme d'amélioration de l'expérience utilisateur Windows », page 80.

Procédure

1 Désinstallez Tablet PC Components, à moins que cette fonction soit requise.

2 Désactivez IPv6, sauf si l'option est requise.

3 Utilisez la commande de l'utilitaire du système de fichiers (`fsutil`) pour désactiver le paramètre qui archive l'heure du dernier accès à un fichier.

   Par exemple : `fsutil behavior set disablelastaccess 1`

4 Démarrez l'éditeur de Registre (`regedit.exe`) et remplacez la valeur de la clé **[TimeOutValue]** REG_DWORD, dans le chemin `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Disk`, par **`0x000000be(190)`**.

5 Désactivez le programme d'amélioration de l'expérience utilisateur Windows et les tâches liées du Planificateur de tâches.

6 Arrêtez le système d'exploitation client et éteignez la machine virtuelle.

7 Activez la machine virtuelle.

Suivant

Reportez-vous à la section « Optimisation de Windows 7 et Windows 8 pour les postes de travail de clone lié », page 81 pour obtenir plus d'informations sur la désactivation de certains services et tâches de Windows 7 et Windows 8, afin de réduire la croissance de postes de travail de clone lié View Composer. La désactivation de certains services et tâches peut également entraîner une amélioration des performances sur les machines virtuelles complètes.

Désactiver le programme d'amélioration de l'expérience utilisateur Windows

La désactivation du programme d'amélioration de l'expérience utilisateur Windows et les tâches du Planificateur de tâches liées qui contrôlent ce programme peuvent améliorer les performances des système Windows 7 et Windows 8 dans les pools de postes de travail View volumineux.

Procédure

1 Dans le système d'exploitation client Windows 7 ou Windows 8, démarrez le panneau de configuration et cliquez sur **[Centre de maintenance] > [Modifier les paramètres du Centre de maintenance]** .

2 Cliquez sur **[Paramètres du programme d'amélioration de l'expérience utilisateur]** .

3 Sélectionnez **[Non, je ne veux pas participer au programme]** et cliquez sur **[Enregistrer les modifications]** .

4 Démarrez le panneau de configuration et cliquez sur **[Outils d'administration] > [Planificateur de tâches]** .

5 Dans le volet Planificateur de tâches (local) de la boîte de dialogue Planificateur de tâches, développez les nœuds **[Bibliothèque du Planificateur de tâches] > [Microsoft] > [Windows]** et ouvrez le dossier **[Application Experience]** .

6 Désactivez les tâches **[AITAgent]** et **[ProgramDataUpdater]** .

7 Dans le nœud **[Bibliothèque du Planificateur de tâches] > [Microsoft] > [Windows]** , ouvrez le dossier **[Customer Experience Improvement Program]** .

8 Désactivez les tâches **[Consolidator]** , **[KernelCEIPTask]** et **[UsbCEIP]** .

Suivant

Réalisez d'autres tâches d'optimisation de Windows 7 ou Windows 8. Reportez-vous à la section « Optimiser les performances du système d'exploitation client Windows 7 et Windows 8 », page 80.

Optimisation de Windows 7 et Windows 8 pour les postes de travail de clone lié

En désactivant certains services et tâches de Windows 7 ou Windows 8, vous pouvez réduire la croissance de postes de travail de clone lié View Composer. La désactivation de certains services et tâches peut également entraîner une amélioration des performances sur les machines virtuelles complètes.

Avantages de la désactivation des services et tâches Windows 7 et Windows 8

Windows 7 et Windows 8 planifient des services et des tâches qui peuvent entraîner la croissance de clones liés de View Composer, même lorsque les postes de travail de clone lié sont inactifs. La croissance incrémentielle de disques du système d'exploitation de clone lié peut annuler les économies de stockage que vous atteignez lorsque vous créez les postes de travail de clone lié. Vous pouvez réduire la croissance de clone lié en désactivant ces services Windows.

Windows 7 et Windows 8 contiennent de nouveaux services et planifient des services plus anciens à exécuter par défaut, tels que la défragmentation de disque. Ces services s'exécutent dans l'arrière-plan si vous ne les désactivez pas.

Les services qui affectent la croissance du disque du système d'exploitation génèrent également des opérations d'entrée/sortie par seconde (IOPS) sur les machines virtuelles Windows 7 ou Windows 8. La désactivation de ces services peut réduire l'IOPS et améliorer les performances sur des machines virtuelles complètes et des clones liés.

La désactivation de certains services peut également avantager des systèmes d'exploitation Windows XP et Windows Vista.

Ces meilleures pratiques pour l'optimisation de Windows 7 et Windows 8 s'appliquent à la plupart des environnements d'utilisateur. Toutefois, vous devez évaluer l'effet de la désactivation de chaque service sur vos utilisateurs, applications et postes de travail. Il peut être nécessaire de laisser certains services actifs.

Par exemple, la désactivation du service Windows Update est utile si vous actualisez et recomposez les postes de travail de clone lié. Une opération d'actualisation restaure les disques du système d'exploitation sur leurs derniers snapshots, ce qui supprime toutes les mises à jour Windows automatiques depuis la prise des derniers snapshots. Une opération de recomposition recrée les disques du système d'exploitation à partir d'un nouveau snapshot pouvant contenir les mises à jour Windows actuelles, ce qui rend les mises à jour Windows automatiques redondantes.

Si vous n'utilisez pas l'actualisation et la recomposition régulièrement, vous pouvez décider de laisser le service Windows Update actif.

Présentation des services et tâches Windows 7 et Windows 8 qui entraînent la croissance de clone lié

Certains services et tâches Windows 7 et Windows 8 peuvent entraîner la croissance incrémentielle de disques du système d'exploitation de clone lié après quelques heures, même lorsque les postes de travail de clone lié sont inactifs. Si vous désactivez ces services et tâches, vous pouvez contrôler la croissance du disque du système d'exploitation.

Les services qui affectent la croissance du disque du système d'exploitation génèrent également des IOPS sur les machines virtuelles Windows 7 et Windows 8. Vous pouvez évaluer les avantages de la désactivation de ces services sur des machines virtuelles complètes ainsi que sur des clones liés.

Avant de désactiver les services Windows 7 ou Windows 8 indiqués dans le Tableau 4-7, vérifiez que vous avez effectué les étapes d'optimisation dans la section « Optimiser les performances du système d'exploitation Windows client », page 78 et « Optimiser les performances du système d'exploitation client Windows 7 et Windows 8 », page 80.

Tableau 4-7. Impact des services et tâches Windows 7 et Windows 8 sur la croissance du disque du système d'exploitation et l'IOPS lorsque le système d'exploitation est laissé inactif

Service ou tâche	Description	Occurrence par défaut ou démarrage	Impact sur les disques du système d'exploitation de clone lié	Impact sur l'IOPS	Désactiver ce service ou tâche ?
Mise en veille prolongée Windows	Offre un état d'économie d'énergie en stockant des documents et des programmes ouverts dans un fichier avant que l'ordinateur ne soit désactivé. Le fichier est rechargé dans la mémoire lorsque l'ordinateur est redémarré, en restaurant l'état au moment où la mise en veille prolongée a été appelée.	Les paramètres par défaut du mode de gestion de l'alimentation désactivent la mise en veille prolongée.	Élevé. Par défaut, la taille du fichier de mise en veille prolongée, `hiberfil.sys`, est la même que la RAM installée sur la machine virtuelle. Cette fonction affecte tous les systèmes d'exploitation client.	Élevé. Lorsque la mise en veille prolongée est déclenchée, le système écrit un fichier `hiberfil.sys` de la taille de la RAM installée.	Oui La mise en veille prolongée n'a aucun avantage dans un environnement virtuel. Pour plus d'informations, reportez-vous à la section « Désactiver la mise en veille prolongée Windows sur la machine virtuelle parente », page 92..
Défragmentation de disque planifiée Windows	La défragmentation de disque est planifiée en tant que processus d'arrière-plan.	Une fois par semaine	Élevé. Des opérations de défragmentation répétées peuvent augmenter de plusieurs Go la taille des disques du système d'exploitation de clone lié et ne rendent pas l'accès au disque plus efficace sur les clones liés.	Élevée	Oui

Tableau 4-7. Impact des services et tâches Windows 7 et Windows 8 sur la croissance du disque du système d'exploitation et l'IOPS lorsque le système d'exploitation est laissé inactif (suite)

Service ou tâche	Description	Occurrence par défaut ou démarrage	Impact sur les disques du système d'exploitation de clone lié	Impact sur l'IOPS	Désactiver ce service ou tâche ?
Service Windows Update	Détecte, télécharge et installe des mises à jour pour Windows et d'autres programmes.	Démarrage automatique	Moyen à élevé. Entraîne des écritures fréquentes sur les disques du système d'exploitation des clones liés car des vérifications de mise à jour se produisent souvent. L'impact dépend des mises à jour téléchargées.	Moyen à élevé	Oui, si vous utilisez la recomposition de View Composer pour installer des mises à jour Windows et l'actualisation pour remettre les disques du système d'exploitation à leurs snapshots d'origine.
Service de stratégie de diagnostic Windows	Détecte, dépanne et résout des problèmes liés aux composants Windows. Si vous arrêtez ce service, les diagnostics ne fonctionnent plus.	Démarrage automatique	Moyen à élevé. Le service est déclenché à la demande. La fréquence d'écriture varie, en fonction de la demande.	Faible à moyen	Oui, si vous n'avez pas besoin que les outils de diagnostic fonctionnent sur les postes de travail.
Prérécupération/Superfetch	Stocke des informations spécifiques sur les applications que vous exécutez pour les aider à démarrer plus vite. Cette fonction a été présentée dans Windows XP.	Toujours activé, sauf s'il est désactivé.	Moyenne Entraîne des mises à jour périodiques de ses informations de disposition et de base de données et des fichiers de prérécupération individuels, qui sont générés à la demande.	Moyenne	Oui, si les heures de démarrage d'application sont acceptables quand vous désactivez cette fonction.
Sauvegarde du registre Windows (`RegIdleBackup`)	Sauvegarde automatiquement le registre Windows lorsque le système est inactif.	Tous les 10 jours à minuit	Moyen. Chaque fois que cette tâche s'exécute, elle génère des fichiers de sauvegarde de registre.	Moyen.	Oui. La sauvegarde du registre Windows n'est pas nécessaire. Pour restaurer des données de registre, vous pouvez utiliser l'opération d'actualisation de View Composer.
Restauration du système	Rétablit le système Windows à un état d'intégrité précédent.	Lorsque Windows démarre et ensuite une fois par jour.	Faible à moyen. Capture un point de restauration système dès que le système détecte qu'il est nécessaire. Lorsque le clone lié est inactif, ce temps système est faible.	Aucun impact majeur.	Oui Bien que son impact soit faible, cette tâche est redondante si vous utilisez l'actualisation de View Composer pour rétablir des disques du système d'exploitation à leurs snapshots d'origine.

Tableau 4-7. Impact des services et tâches Windows 7 et Windows 8 sur la croissance du disque du système d'exploitation et l'IOPS lorsque le système d'exploitation est laissé inactif (suite)

Service ou tâche	Description	Occurrence par défaut ou démarrage	Impact sur les disques du système d'exploitation de clone lié	Impact sur l'IOPS	Désactiver ce service ou tâche ?
Windows Defender	Offre des fonctions anti-espion.	Au démarrage de Windows. Effectue une analyse rapide une fois par jour. Recherche des mises à jour avant chaque analyse.	Moyen à élevé. Effectue des mises à jour de définition, des analyses planifiées et des analyses démarrées à la demande.	Moyen à élevé.	Oui, si un autre logiciel anti-espion est installé.
Tâche Microsoft Feeds Synchronization (`msfeedssync.exe`)	Met à jour périodiquement des flux RSS dans les navigateurs Windows Internet Explorer. Cette tâche met à jour des flux RSS pour lesquels la synchronisation de flux RSS automatique est activée. Le processus apparaît dans le Gestionnaire des tâches de Windows uniquement quand Internet Explorer est en cours d'exécution.	Une fois par jour.	Moyen. Affecte la croissance du disque du système d'exploitation si aucun disque persistant n'est configuré. Si des disques persistants sont configurés, l'impact est dévié sur les disques persistants.	Moyenne	Oui, si vos utilisateurs ne requièrent pas de mises à jour RSS automatiques sur leurs postes de travail.

Désactiver la défragmentation de disque planifiée sur des machines virtuelles parentes Windows 7 et Windows 8

Avant de créer des clones liés, vous devez désactiver les défragmentations planifiées sur des machines virtuelles parentes Windows 7 et Windows 8. Par défaut, Windows 7 et Windows 8 planifient des défragmentations de disque une fois par semaine. Des opérations de défragmentation répétées augmentent significativement la taille des disques du système d'exploitation de clone lié et ne rendent pas l'accès au disque plus efficace sur les clones liés.

Lorsque vous créez un pool de clone lié à partir de la machine virtuelle parente, les clones liés partagent le disque du réplica. Les opérations de défragmentation suivantes n'affectent pas le disque du réplica, qui est en lecture seule. Au lieu de cela, les défragmentations développent le disque du système d'exploitation de chaque clone.

Il est recommandé de défragmenter la machine virtuelle parente une fois, avant de prendre un snapshot et de créer le pool. Les clones liés bénéficient de la défragmentation car ils partagent le disque optimisé en lecture seule du réplica.

Prérequis

- Vérifiez que les applications que vous prévoyez de déployer sur les clones liés sont installés sur la machine virtuelle.
- Vérifiez que View Agent avec View Composer Agent est installé sur la machine virtuelle.

Procédure

1 Dans vSphere Client, sélectionnez la machine virtuelle parente et sélectionnez **[Ouvrir la console]** .

2 Ouvrez une session sur le système d'exploitation client Windows 7 ou Windows 8 en tant qu'administrateur.

3 Cliquez sur **[Démarrer]** et saisissez **`defrag`** dans la zone **[Rechercher les programmes et fichiers]** .

4 Dans le volet Programmes, cliquez sur **[Défragmenteur de disque]** .

5 Dans la boîte de dialogue **[Défragmenteur de disque]** , cliquez sur **[Défragmenter le disque]** .

Le Défragmenteur de disque consolide les fichiers défragmentés sur le disque dur de la machine virtuelle.

6 Dans la boîte de dialogue **[Défragmenteur de disque]** , cliquez sur **[Configurer la planification]** .

7 Décochez la case **[Exécution planifiée (recommandé)]** et cliquez sur **[OK]** .

Les opérations de défragmentation n'auront pas lieu sur des machines virtuelles de clone lié créées à partir de cette machine virtuelle parente.

Désactiver le service Windows Update sur des machines virtuelles Windows 7 et Windows 8

La désactivation du service Windows Update peut réduire le nombre de fichiers créés et les écritures se produisant lorsque des mises à jour sont téléchargées et installées. Cette action peut réduire la croissance de clone lié et réduire l'IOPS dans des clones liés et des machines virtuelles complètes.

Désactivez le service Windows Update si vous actualisez et recomposez les postes de travail de clone lié. Une opération d'actualisation restaure les disques du système d'exploitation à leurs snapshots d'origine, en supprimant les mises à jour Windows automatiques. Une opération de recomposition recrée les disques du système d'exploitation à partir d'un nouveau snapshot pouvant contenir des mises à jour Windows, ce qui rend les mises à jour Windows automatiques redondantes.

Ne désactivez pas le service Windows Update si vous n'utilisez pas la recomposition pour installer des mises à jour Windows dans les clones liés.

Prérequis

Vérifiez que les mises à jour Windows les plus récentes sont téléchargées et installées sur la machine virtuelle.

Procédure

1 Dans vSphere Client, sélectionnez la machine virtuelle parente et sélectionnez **[Ouvrir la console]** .

2 Ouvrez une session sur le système d'exploitation client Windows 7 ou Windows 8 en tant qu'administrateur.

3 Cliquez sur **[Démarrer] > [Panneau de configuration] > [Système et sécurité] > [Activer ou désactiver la mise à jour automatique]** .

4 Dans le menu Mises à jour importantes, sélectionnez **[Ne jamais rechercher de mises à jour]** .

5 Décochez la case **[Recevoir les mises à jour recommandées de la même façon que vous recevez les mises à jour importantes]** .

6 Décochez la case **[Autoriser tous les utilisateurs à installer les mises à jour sur cet ordinateur]** et cliquez sur **[OK]** .

Désactiver le service de stratégie de diagnostic sur des machines virtuelles Windows 7 et Windows 8

La désactivation du service de stratégie de diagnostic Windows peut réduire le nombre d'écritures système et diminuer la croissance des postes de travail de clone lié.

Ne désactivez pas le service de stratégie de diagnostic Windows si vos utilisateurs ont besoin des outils de diagnostic sur leurs postes de travail.

Procédure

1 Dans vSphere Client, sélectionnez la machine virtuelle parente et sélectionnez **[Ouvrir la console]** .

2 Ouvrez une session sur le système d'exploitation client Windows 7 ou Windows 8 en tant qu'administrateur.

3 Cliquez sur **[Démarrer] > [Panneau de configuration] > [Système et sécurité] > [Outils d'administration]** .

4 Sélectionnez **[Services]** et cliquez sur **[Ouvrir]** .

5 Double-cliquez sur **[Service de stratégie de diagnostic]** .

6 Dans la boîte de dialogue Propriétés du service de stratégie de diagnostic (Ordinateur local), cliquez sur **[Arrêter]** .

7 Dans le menu Type de démarrage, sélectionnez **[Désactivé]** .

8 Cliquez sur **[OK]** .

Désactiver les fonctions de prérécupération et Superfetch sur des machines virtuelles Windows 7 et Windows 8

En désactivant les fonctions de prérécupération et Superfetch de Windows, vous pouvez éviter de générer des fichiers de prérécupération et le temps système associé aux opérations de prérécupération et Superfetch. Cette action peut réduire la croissance des postes de travail de clone lié et réduire l'IOPS sur des machines virtuelles complètes et des clones liés.

Pour désactiver les fonctions de prérécupération et Superfetch, vous devez modifier une clé de Registre Windows et désactiver le service de prérécupération sur la machine virtuelle.

Prérequis

Pour plus d'informations sur l'utilisation de l'éditeur de Registre Windows sous Windows 7 et Windows 8, consultez le site Web Microsoft TechNet.

Procédure

1 Démarrez l'éditeur de Registre Windows sur la machine virtuelle Windows 7 ou Windows 8 locale.

2 Allez à la clé de Registre appelée **[PrefetchParameters]** .

La clé de Registre se trouve à l'emplacement suivant : `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters`.

3 Définissez les valeurs **[EnablePrefetcher]** et **[EnableSuperfetch]** sur `0`.

4 Cliquez sur **[Démarrer] > [Panneau de configuration] > [Système et sécurité] > [Outils d'administration]** .

5 Sélectionnez **[Services]** et cliquez sur **[Ouvrir]** .

6 Double-cliquez sur le service **[Superfetch]** .

7 Dans la boîte de dialogue Propriétés de Superfetch (Ordinateur local), cliquez sur **[Arrêter]** .

8 Dans le menu Type de démarrage, sélectionnez **[Désactivé]** .

9 Cliquez sur **[OK]** .

Désactiver la sauvegarde du Registre Windows sur des machines virtuelles Windows 7 et Windows 8

La désactivation de la fonction de sauvegarde du Registre Windows, `RegIdleBackup`, peut réduire le nombre d'écritures système et diminuer la croissance des postes de travail de clone lié.

Procédure

1 Dans vSphere Client, sélectionnez la machine virtuelle parente et sélectionnez **[Ouvrir la console]** .

2 Ouvrez une session sur le système d'exploitation client Windows 7 ou Windows 8 en tant qu'administrateur.

3 Cliquez sur **[Démarrer]** > **[Panneau de configuration]** > **[Système et sécurité]** > **[Outils d'administration]** .

4 Sélectionnez **[Planificateur de tâches]** et cliquez sur **[Ouvrir]** .

5 Dans le volet de gauche, développez **[Bibliothèque du Planificateur de tâches]** , **[Microsoft]** , **[Windows]** .

6 Double-cliquez sur **[Registry]** et sélectionnez **[RegIdleBackup]** .

7 Dans le volet Actions, cliquez sur **[Désactiver]** .

Désactiver la Restauration du système sur des machines virtuelles Windows 7 et Windows 8

Vous n'avez pas à utiliser la fonction de Restauration du système Windows si vous utilisez l'actualisation de View Composer pour restaurer des disques du système d'exploitation de clone lié sur leurs snapshots d'origine.

Lorsque le système d'exploitation est inactif, la Restauration du système n'a pas un impact visible sur la croissance du disque du système d'exploitation. Toutefois, lorsque le système d'exploitation est utilisé, la Restauration du système génère des points de restauration basés sur l'utilisation du système, ce qui a un impact important sur la croissance du disque du système d'exploitation.

La fonction de Restauration du système Windows est la même que l'actualisation de View Composer.

Il est recommandé de désactiver la Restauration du système Windows et d'éviter une croissance inutile dans vos clones liés.

Si vous n'utilisez pas l'actualisation, évaluez s'il est plus utile de laisser la Restauration du système active dans votre environnement View.

Procédure

1 Dans vSphere Client, sélectionnez la machine virtuelle parente et sélectionnez **[Ouvrir la console]** .

2 Ouvrez une session sur le système d'exploitation client Windows 7 ou Windows 8 en tant qu'administrateur.

3 Cliquez sur **[Démarrer]** > **[Panneau de configuration]** > **[Système et sécurité]** > **[Outils d'administration]** .

4 Sélectionnez **[Planificateur de tâches]** et cliquez sur **[Ouvrir]** .

5 Dans le volet de gauche, développez **[Bibliothèque du Planificateur de tâches]** , **[Microsoft]** , **[Windows]** .

6 Double-cliquez sur **[SystemRestore]** et sélectionnez **[SR]** .

7 Dans le volet Actions, cliquez sur **[Désactiver]** .

Désactiver Windows Defender sur des machines virtuelles Windows 7 et Windows 8

Microsoft Windows Defender peut contribuer à la croissance du disque du système d'exploitation de clone lié et à l'augmentation de l'IOPS dans des clones liés et des machines virtuelles complètes. Désactivez Windows Defender si vous installez un autre logiciel anti-espion sur la machine virtuelle.

Si Windows Defender est le seul anti-espion installé sur la machine virtuelle, vous pouvez préférer laisser Windows Defender actif sur les postes de travail dans votre environnement.

Procédure

1 Dans vSphere Client, sélectionnez la machine virtuelle parente et sélectionnez **[Ouvrir la console]** .

2 Ouvrez une session sur le système d'exploitation client Windows 7 ou Windows 8 en tant qu'administrateur.

3 Cliquez sur **[Démarrer]** et saisissez `Windows Defender` dans la zone Rechercher les programmes et fichiers.

4 Cliquez sur **[Outils]** > **[Options]** > **[Administrateur]** .

5 Décochez la case **[Utiliser ce programme]** et cliquez sur **[Enregistrer]** .

Désactiver la tâche Microsoft Feeds Synchronization sur des machines virtuelles Windows 7 et Windows 8

Windows Internet Explorer utilise la tâche Microsoft Feeds Synchronization pour mettre à jour des flux RSS dans les navigateurs Web des utilisateurs. Cette tâche peut contribuer à la croissance de clone lié. Désactivez cette tâche si vos utilisateurs n'ont pas besoin de mises à jour automatiques des flux RSS dans leurs navigateurs.

Microsoft Feeds Synchronization peut entraîner la croissance du disque du système d'exploitation si aucun disque persistant n'est configuré. Si des disques persistants sont configurés, l'impact est dévié sur les disques persistants. Dans cette situation, vous devez toujours désactiver Microsoft Feeds Synchronization pour contrôler la croissance de disque persistant.

Procédure

1 Dans vSphere Client, sélectionnez la machine virtuelle parente et sélectionnez **[Ouvrir la console]** .

2 Ouvrez une session sur le système d'exploitation client Windows 7 ou Windows 8 en tant qu'administrateur.

3 Cliquez sur **[Démarrer]** > **[Panneau de configuration]** > **[Réseau et Internet]** > **[Options Internet]** .

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

5 Flux et composants Web Slice, cliquez sur **[Paramètres]** .

6 Décochez la case **[Rechercher automatiquement les mises à jour des flux et des composants Web Slice]** et cliquez sur **[OK]** .

7 Dans la boîte de dialogue Propriétés Internet, cliquez sur **[OK]** .

Préparation de machines virtuelles pour View Composer

Pour déployer des postes de travail de clone lié, vous devez préparer une machine virtuelle parente qui satisfait les exigences du service View Composer.

- Préparer une machine virtuelle parente page 89

  Le service View Composer requiert une machine virtuelle parente à partir de laquelle vous générez une image de base pour créer et gérer des postes de travail de clone lié.

- Activation de Windows sur des postes de travail de clone lié page 91

  Pour vous assurer que View Composer active correctement les systèmes d'exploitation Windows 8, Windows 7 et Windows Vista sur des postes de travail de clone lié, vous devez utiliser l'activation du volume Microsoft sur la machine virtuelle parente. La technologie d'activation du volume requiert une clé de licence en volume.

- Désactiver la mise en veille prolongée Windows sur la machine virtuelle parente page 92

  L'option de mise en veille prolongée Windows crée un fichier système volumineux qui peut augmenter la taille des disques du système d'exploitation de clone lié créés à partir de la machine virtuelle parente. La désactivation de l'option de mise en veille prolongée réduit la taille des clones liés.

- Configurer une machine virtuelle parente pour utiliser le stockage local page 93

  Lorsque vous préparez une machine virtuelle parente pour View Composer, vous pouvez configurer la machine virtuelle parente et des postes de travail de clone lié pour stocker des fichiers d'échange de machine virtuelle sur le magasin de données local. Cette stratégie facultative vous permet de bénéficier du stockage local.

- Conserver une trace de la taille du fichier d'échange de la machine virtuelle parente page 94

  Lorsque vous créez un pool de clone lié, vous pouvez rediriger les fichiers d'échange et temporaires du système d'exploitation client des clones liés vers un disque séparé. Vous devez configurer ce disque pour qu'il soit plus volumineux que le fichier d'échange sur le système d'exploitation client.

- Augmenter la limite du délai d'expiration des scripts de personnalisation QuickPrep page 95

  View Composer termine un script de post-synchronisation ou de désactivation QuickPrep qui prend plus de 20 secondes. Vous pouvez augmenter la limite du délai d'expiration de ces scripts en modifiant la valeur de registre Windows `ExecScriptTimeout` sur la machine virtuelle parente.

Préparer une machine virtuelle parente

Le service View Composer requiert une machine virtuelle parente à partir de laquelle vous générez une image de base pour créer et gérer des postes de travail de clone lié.

Prérequis

- Vérifiez que vous avez préparé une machine virtuelle à utiliser pour le déploiement de postes de travail View. Reportez-vous à la section « Création de machines virtuelles pour un déploiement de poste de travail View », page 65.

Une machine virtuelle parente que vous utilisez pour View Composer doit appartenir au même domaine Active Directory que le domaine que les postes de travail de clone lié rejoindront ou doit être un membre du Groupe de travail local.

Important Pour utiliser des fonctions prises en charge dans View Manager 4.5 ou supérieur, telles que la redirection de données supprimables sur un disque séparé et la personnalisation de postes de travail de clone lié avec Sysprep, vous devez déployer les postes de travail à partir d'une machine virtuelle parente sur laquelle View Agent 4.5 ou supérieur est installé.

Vous ne pouvez pas utiliser View Composer pour déployer des postes de travail qui exécutent Windows Vista Ultimate Edition ou Windows XP Professional SP1.

- Vérifiez que la machine virtuelle n'a pas été convertie depuis un clone lié View Composer. Une machine virtuelle convertie depuis un clone lié contient les informations de disque interne et d'état du clone. Une machine virtuelle parente ne peut pas contenir d'informations d'état.

  Important Les clones liés et les machines virtuelles qui ont été convertis depuis des clones liés ne sont pas pris en charge en tant que machines virtuelles parentes.

- Si la machine virtuelle parente s'exécute sous Windows XP, et qu'Active Directory s'exécute sous Windows Server 2008, appliquez un correctif de mise à jour sur la machine virtuelle Windows XP. Consultez l'article 944043 du support Microsoft à l'adresse suivante : http://support.microsoft.com/kb/944043/en-us.

  Si vous n'installez pas le pack de compatibilité du contrôleur de domaine en lecture seule (RODC) Windows Server 2008 pour Windows XP, les clones liés déployés à partir de cette machine virtuelle parente ne parviennent pas à joindre le domaine.

- Lorsque vous installez View Agent sur la machine virtuelle parente, sélectionnez l'option **[View Composer Agent]** . Reportez-vous à la section « Installer View Agent sur une machine virtuelle », page 71.

  Pour mettre à jour View Agent dans un environnement volumineux, vous pouvez utiliser des mécanismes de mise à jour Windows standard comme Altiris, SMS, LanDesk, BMC ou d'autres logiciels de gestion des systèmes. Vous pouvez également utiliser l'opération de recomposition pour mettre à jour View Agent.

  Remarque Ne modifiez pas le compte d'ouverture de session pour le service VMware View Composer Guest Agent Server dans une machine virtuelle parente. Par défaut, il s'agit du compte de système local. Si vous modifiez ce compte, les clones liés créés à partir du parent ne démarrent pas.

- Pour déployer des postes de travail exécutant Windows 8, Windows 7 ou Windows Vista, configurez une clé de licence en volume et activez le système d'exploitation de la machine virtuelle parente avec l'activation du volume. Reportez-vous à la section « Activation de Windows sur des postes de travail de clone lié », page 91.

- Si la machine virtuelle parente exécute Windows 7 ou Windows 8, vérifiez que vous avez suivi les meilleures pratiques pour optimiser le système d'exploitation. Reportez-vous à la section « Optimisation de Windows 7 et Windows 8 pour les postes de travail de clone lié », page 81.

- Familiarisez-vous avec la procédure de désactivation de la recherche de pilotes de périphérique de Windows Update. Consultez l'article de Microsoft Technet « Désactiver la recherche de pilotes de périphérique de Windows Update » à l'adresse http://technet.microsoft.com/en-us/library/cc730606(v=ws.10).aspx.

Procédure

- Désactivez le bail DHCP sur la machine virtuelle parente pour empêcher la copie d'une adresse IP avec bail vers les clones liés du pool.

  a Sur la machine virtuelle parente, ouvrez une invite de commande.

  b Saisissez la commande **`ipconfig /release`**.

- Vérifiez que le disque système contient un seul volume.

  Vous ne pouvez pas déployer de clones liés à partir d'une machine virtuelle parente contenant plusieurs volumes. Le service View Composer ne prend pas en charge les partitions de disque multiples. Plusieurs disques virtuels sont pris en charge.

  Remarque Si la machine virtuelle parente contient plusieurs disques virtuels, lorsque vous créez un pool de postes de travail, ne sélectionnez pas une lettre de lecteur pour le disque persistant de View Composer ou le disque de données supprimable qui existe déjà sur la machine virtuelle parente ou qui entre en conflit avec une lettre de lecteur utilisée pour un lecteur monté en réseau.

- Vérifiez que la machine virtuelle ne contient pas de disque indépendant.

  Un disque indépendant est exclu lorsque vous prenez un snapshot de la machine virtuelle. Les clones liés qui sont créés ou recomposés à partir de la machine virtuelle ne contiendront pas le disque indépendant.

- Si vous prévoyez de configurer des disques de données supprimables lorsque vous créez des postes de travail de clone lié, supprimez les variables `TEMP` et `TMP` d'utilisateur par défaut de la machine virtuelle parente.

  Vous pouvez également supprimer le fichier `pagefile.sys` pour éviter la duplication du fichier sur tous les clones liés. Si vous laissez le fichier `pagefile.sys` sur la machine virtuelle parente, une version en lecture seule du fichier est héritée par les clones liés, alors qu'une deuxième version du fichier est utilisée sur le disque de données supprimable.

- Désactivez l'option de mise en veille prolongée pour réduire la taille des disques du système d'exploitation de clone lié créés à partir de la machine virtuelle parente.

- Avant de prendre un snapshot de la machine virtuelle parente, désactivez la recherche de pilotes de périphérique de Windows Update.

  Cette fonction Windows peut interférer avec la personnalisation des postes de travail de clone lié. À chaque fois qu'un clone lié est personnalisé, Windows peut rechercher les meilleurs pilotes sur Internet pour ce clone, ce qui entraîne des recherches répétées et des retards de personnalisation.

- Dans vSphere Client, désactivez le paramètre Options vApp sur la machine virtuelle parente.

Vous pouvez déployer un pool de clone lié à partir de la machine virtuelle parente.

Suivant

Utilisez vSphere Client pour prendre un snapshot de la machine virtuelle parente à l'état désactivé. Ce snapshot sert de configuration de ligne de base pour le premier jeu de postes de travail de clone lié ancrés à la machine virtuelle parente.

Important Avant de prendre un snapshot, arrêtez complètement la machine virtuelle parente à l'aide de la commande **[Arrêter]** dans le système d'exploitation client.

Activation de Windows sur des postes de travail de clone lié

Pour vous assurer que View Composer active correctement les systèmes d'exploitation Windows 8, Windows 7 et Windows Vista sur des postes de travail de clone lié, vous devez utiliser l'activation du volume Microsoft sur la machine virtuelle parente. La technologie d'activation du volume requiert une clé de licence en volume.

Pour activer Windows 8, Windows 7 ou Windows Vista avec l'activation du volume, vous utilisez un service de gestion des clés (KMS), qui requiert une clé de licence KMS. Contactez votre revendeur Microsoft pour acquérir une clé de licence en volume et configurer l'activation du volume.

Remarque View Composer ne prend pas en charge la licence MAK (clé d'activation multiple).

Avant de créer des postes de travail de clone lié avec View Composer, vous devez utiliser l'activation du volume pour activer le système d'exploitation sur la machine virtuelle parente.

Remarque Les postes de travail Windows XP avec des licences en volume ne requièrent pas d'activation.

Lors de la création d'un poste de travail de clone lié, et à chaque recomposition du clone lié, l'agent View Composer utilise le serveur KMS de la machine virtuelle parente pour activer le système d'exploitation sur le clone lié.

L'outil QuickPrep de View Composer implémente l'activation comme suit :

1 Il appelle un script pour supprimer l'état de licence existant sur la machine virtuelle de clone lié.

2 Il redémarre le système d'exploitation client.

3 Il appelle un script qui utilise la licence KMS pour activer le système d'exploitation sur le clone.

Chaque fois que QuickPrep s'exécute sur un clone lié, l'activation a lieu.

Pour la licence KMS, View Composer utilise le serveur KMS configuré pour activer la machine virtuelle parente. Le serveur KMS traite un clone lié activé en tant qu'ordinateur avec une nouvelle licence émise.

Désactiver la mise en veille prolongée Windows sur la machine virtuelle parente

L'option de mise en veille prolongée Windows crée un fichier système volumineux qui peut augmenter la taille des disques du système d'exploitation de clone lié créés à partir de la machine virtuelle parente. La désactivation de l'option de mise en veille prolongée réduit la taille des clones liés.

L'option de mise en veille prolongée de Windows crée un fichier système masqué, `Hiberfil.sys`. Windows utilise ce fichier pour stocker une copie de la mémoire système sur le disque dur lorsque le paramètre de veille hybride est activé. Lorsque vous créez un pool de clone lié, le fichier est créé sur le disque du système d'exploitation sur chaque clone lié.

Sur des machines virtuelles Windows 7 ou Windows 8, ce fichier peut atteindre 10 Go.

Avertissement Lorsque vous activez la mise en veille prolongée, le paramètre de veille hybride ne fonctionne pas. Les utilisateurs peuvent perdre des données si le paramètre de veille hybride est activé et qu'une coupure de courant se produit.

Prérequis

Familiarisez-vous avec la fonction de mise en veille prolongée de Windows. Consultez le site Web du support Microsoft. Pour plus d'informations sur la désactivation de la mise en veille prolongée sous Windows 8, Windows 7 ou Windows Vista, consultez le site Web du support Microsoft et recherchez comment désactiver et réactiver la mise en veille prolongée sur un ordinateur exécutant Windows.

Procédure

1 Dans vSphere Client, sélectionnez la machine virtuelle parente et sélectionnez **[Ouvrir la console]** .

2 Ouvrez une session sur le système d'exploitation client Windows en tant qu'administrateur.

3 Désactivez l'option de mise en veille prolongée.

Système d'exploitation	Action
Windows 8, Windows 7 ou Windows Vista	a Cliquez sur **[Démarrer]** et saisissez **cmd** dans la zone **[Démarrer la recherche]** . b Dans la liste de résultats de la recherche, cliquez avec le bouton droit sur **[Invite de commande]** et cliquez sur **[Exécuter en tant qu'administrateur]** . c À l'invite Contrôle de compte d'utilisateur, cliquez sur **[Continuer]** . d À l'invite de commande, saisissez **powercfg.exe /hibernate off** et appuyez sur Entrée. e Saisissez **exit** et appuyez sur Entrée.
Windows XP	a Cliquez sur **[Démarrer]** > **[Exécuter]** . b Saisissez **cmd** et cliquez sur **[OK]** . c À l'invite de commande, saisissez **powercfg.exe /hibernate off** et appuyez sur Entrée. d Saisissez **exit** et appuyez sur Entrée.

4 Fermez la session sur le système d'exploitation client.

Lorsque vous créez des postes de travail de clone lié à partir de la machine virtuelle parente, le fichier `Hiberfil.sys` n'est pas créé sur les disques du système d'exploitation de clone lié.

Configurer une machine virtuelle parente pour utiliser le stockage local

Lorsque vous préparez une machine virtuelle parente pour View Composer, vous pouvez configurer la machine virtuelle parente et des postes de travail de clone lié pour stocker des fichiers d'échange de machine virtuelle sur le magasin de données local. Cette stratégie facultative vous permet de bénéficier du stockage local.

Dans cette procédure, vous configurez le stockage local pour les fichiers d'échange de machine virtuelle, pas les fichiers d'échange et temporaires dans le système d'exploitation client. Lorsque vous créez un pool de clone lié, vous pouvez également rediriger les fichiers d'échange et temporaires du système d'exploitation client vers un disque séparé. Reportez-vous à la section « Feuille de calcul pour créer un pool de postes de travail de clone lié », page 103.

Prérequis

Préparez la machine virtuelle parente pour répondre aux exigences du service View Composer. Reportez-vous à la section « Préparer une machine virtuelle parente », page 89.

Procédure

1 Configurez un magasin de données de fichier d'échange sur l'hôte ou le cluster ESX/ESXi sur lequel vous allez déployer le pool de clone lié.

2 Lorsque vous créez la machine virtuelle parente dans vCenter Server, stockez les fichiers d'échange de machine virtuelle sur le magasin de données de fichier d'échange sur l'hôte ou le cluster ESX/ESXi local :

   a Dans vSphere Client, sélectionnez la machine virtuelle parente.

   b Cliquez sur **[Edit Settings (Modifier les paramètres)]** et cliquez sur l'onglet **[Options]** .

   c Cliquez sur **[Swapfile location (Emplacement du fichier d'échange)]** puis sur **[Store in the host's swapfile datastore (Stocker dans le magasin de données de fichier d'échange de l'hôte)]** .

   Pour plus d'instructions, consultez la documentation de VMware vSphere.

Lorsque vous déployez un pool à partir de cette machine virtuelle parente, les postes de travail de clone lié utilisent le magasin de données de fichier d'échange de l'hôte ESX local.

Conserver une trace de la taille du fichier d'échange de la machine virtuelle parente

Lorsque vous créez un pool de clone lié, vous pouvez rediriger les fichiers d'échange et temporaires du système d'exploitation client des clones liés vers un disque séparé. Vous devez configurer ce disque pour qu'il soit plus volumineux que le fichier d'échange sur le système d'exploitation client.

Lorsqu'un clone lié configuré avec un disque séparé pour les fichiers supprimables est mis hors tension, View Manager remplace le disque temporaire par une copie du disque temporaire d'origine que View Composer a créé avec le pool de clone lié. Cette fonction peut ralentir la croissance des clones liés. Toutefois, cette fonction ne peut agir que si vous configurez le disque de fichier supprimable pour qu'il soit suffisamment volumineux pour contenir les fichiers d'échange du système d'exploitation client.

Avant de configurer le disque de fichier supprimable, vous devez connaître la taille maximale de fichier d'échange dans la machine virtuelle parente. Les clones liés ont la même taille de fichier d'échange que la machine virtuelle parente à partir de laquelle ils sont créés.

Il est recommandé de supprimer le fichier `pagefile.sys` de la machine virtuelle parente avant de prendre un snapshot pour éviter la duplication du fichier sur tous les clones liés. Reportez-vous à la section « Préparer une machine virtuelle parente », page 89.

Remarque Cette fonctionnalité n'est pas la même que la configuration du stockage local pour les fichiers d'échange de machine virtuelle. Reportez-vous à la section « Configurer une machine virtuelle parente pour utiliser le stockage local », page 93.

Procédure

1 Dans vSphere Client, cliquez avec le bouton droit sur la machine virtuelle parente et cliquez sur **[Ouvrir la console]** .

2 Sélectionnez **[Démarrer]** > **[Paramètres]** > **[Panneau de configuration]** > **[Système]** .

3 Cliquez sur l'onglet **[Avancé]** .

4 Dans le volet Performances, cliquez sur **[Paramètres]** .

5 Cliquez sur l'onglet **[Avancé]** .

6 Dans le volet Mémoire virtuelle, cliquez sur **[Modifier]** .

La page Mémoire virtuelle apparaît.

7 Définissez la taille du fichier d'échange sur une valeur supérieure à celle de la mémoire affectée à la machine virtuelle.

Important Si le paramètre **[Taille maximale (Mo)]** est inférieur à la taille de la mémoire de la machine virtuelle, saisissez une valeur supérieure et enregistrez la nouvelle valeur.

8 Conservez une trace du paramètre **[Taille maximale (Mo)]** configuré dans le volet Taille du fichier d'échange pour le lecteur sélectionné.

Suivant

Lorsque vous configurez un pool de clone lié à partir de cette machine virtuelle parente, configurez un disque de fichier supprimable dont la taille est supérieure à celle du fichier d'échange.

Augmenter la limite du délai d'expiration des scripts de personnalisation QuickPrep

View Composer termine un script de post-synchronisation ou de désactivation QuickPrep qui prend plus de 20 secondes. Vous pouvez augmenter la limite du délai d'expiration de ces scripts en modifiant la valeur de registre Windows `ExecScriptTimeout` sur la machine virtuelle parente.

La limite augmentée du délai d'expiration est propagée aux clones liés créés à partir de la machine virtuelle parente. Les scripts de personnalisation QuickPrep peuvent s'exécuter sur les clones liés à l'heure que vous spécifiez.

Vous pouvez également utiliser votre script de personnalisation pour lancer un autre script ou processus exécutant la longue tâche.

Remarque La plupart des scripts de personnalisation QuickPrep peuvent arrêter leur exécution dans la limite de 20 secondes. Testez vos scripts avant d'augmenter la limite.

Prérequis

- Installez View Agent avec l'option **[View Composer Agent]** sur la machine virtuelle parente.
- Vérifiez que la machine virtuelle parente est préparée pour créer un pool de clone lié. Reportez-vous à la section « Préparer une machine virtuelle parente », page 89.

Procédure

1 Sur la machine virtuelle parente, démarrez l'Éditeur du Registre Windows.

   a Sélectionnez **[Start (Démarrer)]** > **[Command Prompt (Invite de commande)]** .

   b À l'invite de commande, saisissez **[regedit]** .

2 Dans le Registre Windows, recherchez la clé de registre `vmware-viewcomposer-ga`.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\vmware-viewcomposer-ga
```

3 Cliquez sur **[Edit (Modifier)]** et modifiez la valeur de registre.

```
Value Name: ExecScriptTimeout
Value Type: REG_DWORD
Value unit: milliseconds
```

   La valeur par défaut est de 20 000 millisecondes.

La valeur du délai d'expiration est augmentée. Vous n'avez pas à redémarrer Windows pour que cette valeur prenne effet.

Suivant

Prenez un snapshot de la machine virtuelle parente et créez un pool de clone lié.

Création de modèles de machine virtuelle

Vous devez créer un modèle de machine virtuelle avant de pouvoir créer un pool automatisé qui contient des machines virtuelles complètes.

Un modèle de machine virtuelle est une copie principale d'une machine virtuelle pouvant être utilisée pour créer et approvisionner de nouvelles machines virtuelles. En général, un modèle inclut un système d'exploitation client installé et un jeu d'applications.

Vous créez des modèles de machines virtuelles dans vSphere Client. Vous pouvez créer un modèle de machine virtuelle depuis une machine virtuelle configurée précédemment, ou vous pouvez convertir une machine virtuelle configurée précédemment en modèle de machine virtuelle.

Pour plus d'informations sur l'utilisation de vSphere Client pour créer des modèles de machines virtuelles, consultez le guide *vSphere Basic System Administration (Administration de système de base vSphere)*. Pour plus d'informations sur la création de pools automatisés, reportez-vous à la section « Pools automatisés contenant des machines virtuelles complètes », page 98.

Remarque Vous ne créez pas de pool de clone lié depuis un modèle de machine virtuelle.

Création de spécifications de personnalisation

Les spécifications de personnalisation sont facultatives, mais elles peuvent faciliter considérablement les déploiements de pools automatisés en fournissant des informations de configuration de propriétés générales, telles que des paramètres de licence, d'association de domaines et de protocole DHCP.

Avec les spécifications de personnalisation, vous pouvez personnaliser les postes de travail View créés dans View Administrator. Vous créez de nouvelles spécifications de personnalisation en utilisant l'assistant Spécification de personnalisation dans vSphere Client. Vous pouvez également utiliser l'assistant Spécification de personnalisation pour importer des fichiers `sysprep.ini` personnalisés existants.

Pour plus d'informations sur l'utilisation de l'assistant Spécification de personnalisation, consultez le document *vSphere Virtual Machine Administration (Administration de machine virtuelle vSphere)*.

Assurez-vous que les spécifications de personnalisation sont exactes avant de les utiliser dans View Administrator. Dans vSphere Client, déployez et personnalisez une machine virtuelle depuis votre modèle à l'aide des spécifications de personnalisation. Testez entièrement la machine virtuelle, notamment DHCP et l'authentification, avant de créer des postes de travail View.

Remarque Pour appliquer des spécifications de personnalisation à des pools de postes de travail qui utilisent Windows XP, vous devez installer des outils Microsoft Sysprep sur votre machine vCenter Server.

Vous n'avez pas à installer des outils Sysprep dans vCenter Server pour les pools de postes de travail qui utilisent Windows 8, Windows 7 ou Vista. Les outils Sysprep sont intégrés à ces systèmes d'exploitation.

Lorsque vous utilisez une spécification de personnalisation Sysprep pour associer un poste de travail Windows 8 ou Windows 7 à un domaine, vous devez utiliser le nom de domaine complet (FQDN) du domaine Active Directory. Vous ne pouvez pas utiliser le nom NetBIOS du domaine Active Directory.

Création de pools de postes de travail 5

Avec View Manager, vous créez des pools de postes de travail qui fournissent un accès au poste de travail View à des clients. View Manager déploie des pools depuis des sources de postes de travail, qui peuvent être des machines virtuelles gérées par vCenter Server, des machines virtuelles exécutées sur une autre plate-forme de virtualisation, ou des ordinateurs physiques, des serveurs Terminal Server ou des PC lame.

Vous pouvez créer plusieurs types de pools de postes de travail. Vous pouvez également approvisionner un poste de travail individuel en déployant un pool manuel avec une source de postes de travail unique.

- Pools automatisés contenant des machines virtuelles complètes page 98

  Pour créer un pool de postes de travail automatisé, View Manager approvisionne dynamiquement des postes de travail en fonction de paramètres que vous appliquez au pool. View Manager utilise un modèle de machine virtuelle en tant que source de postes de travail pour le pool et crée une nouvelle machine virtuelle dans vCenter Server pour chaque poste de travail.

- Pools de postes de travail de clone lié page 103

  Pour créer un pool de postes de travail de clone lié, View Composer génère des machines virtuelles de clone lié depuis un snapshot d'une machine virtuelle parente. View Manager approvisionne dynamiquement les postes de travail de clone lié en fonction des paramètres que vous appliquez au pool.

- Pools de postes de travail manuels page 136

  Pour créer un pool de postes de travail manuel, View Manager approvisionne des postes de travail depuis des sources de postes de travail existantes. Vous sélectionnez une source de poste de travail distincte pour chaque poste de travail du pool.

- Pools Microsoft Terminal Services page 141

  Vous pouvez utiliser des serveurs Microsoft Terminal Server pour fournir des sessions Terminal Services en tant que postes de travail à des clients View. View Manager gère les sessions Terminal Services de la même façon qu'il gère d'autres postes de travail View.

- Approvisionnement de pools de postes de travail page 143

  Lorsque vous créez un pool de postes de travail, vous sélectionnez des options de configuration qui déterminent la façon dont le pool est géré et comment les utilisateurs interagissent avec les postes de travail.

- Définition de règles d'alimentation pour des pools de postes de travail page 161

  Vous pouvez configurer une règle d'alimentation pour les machines virtuelles d'un pool de postes de travail si les machines virtuelles sont gérées par vCenter Server.

- Configurer View Storage Accelerator pour des pools de postes de travail page 167

  Vous pouvez configurer des pools de postes de travail afin de permettre aux hôtes ESXi de mettre en cache des données de disque de machine virtuelle. Cette fonction, appelée View Storage Accelerator, utilise la fonction CBRC (Content Based Read Cache) dans les hôtes ESXi. View Storage Accelerator peut réduire l'IOPS et améliorer les performances au cours de tempêtes de démarrage, lorsque plusieurs postes

de travail démarrent ou exécutent des analyses antivirus simultanément. La fonction est également utile lorsque des administrateurs ou des utilisateurs chargent des applications ou des données fréquemment. Pour utiliser cette fonction, vous devez vérifier que View Storage Accelerator est activé pour les pools de postes de travail individuels.

- Déploiement de pools de postes de travail volumineux page 169

  Lorsque de nombreux utilisateurs requièrent la même image de poste de travail, vous pouvez créer un pool automatisé volumineux à partir d'un modèle ou d'une machine virtuelle parente. En utilisant une seule image de base et un seul nom de pool, vous pouvez éviter de diviser les postes de travail arbitrairement en plus petits groupes qui doivent être gérés séparément. Cette stratégie simplifie vos tâches de déploiement et d'administration de View.

Pools automatisés contenant des machines virtuelles complètes

Pour créer un pool de postes de travail automatisé, View Manager approvisionne dynamiquement des postes de travail en fonction de paramètres que vous appliquez au pool. View Manager utilise un modèle de machine virtuelle en tant que source de postes de travail pour le pool et crée une nouvelle machine virtuelle dans vCenter Server pour chaque poste de travail.

Feuille de calcul pour créer un pool automatisé contenant des machines virtuelles complètes

Lorsque vous créez un pool de postes de travail automatisé, l'assistant Ajouter un pool de View Administrator vous invite à configurer certaines options. Utilisez cette feuille de calcul pour préparer vos options de configuration avant de créer le pool.

Vous pouvez imprimer cette feuille de calcul et noter les valeurs que vous souhaitez spécifier quand vous exécutez l'assistant Ajouter un pool.

Pour créer un pool de clone lié, reportez-vous à la section « Pools de postes de travail de clone lié », page 103.

Tableau 5-1. Feuille de calcul : options de configuration pour créer un pool automatisé contenant des machines virtuelles complètes

Option	Description	Indiquez votre valeur ici
Affectation d'utilisateur	Choisissez le type d'affectation d'utilisateur : ■ Dans un pool d'affectation dédiée, chaque utilisateur est affecté à un poste de travail. Les utilisateurs reçoivent le même poste de travail chaque fois qu'ils ouvrent une session. ■ Dans un pool d'affectation flottante, les utilisateurs reçoivent différents postes de travail chaque fois qu'ils ouvrent une session. Pour plus d'informations, reportez-vous à la section « Affectation d'utilisateur dans des pools de postes de travail », page 143.	
Activer l'affectation automatique	Dans un pool d'affectation dédiée, un poste de travail est affecté à un utilisateur quand l'utilisateur ouvre d'abord une session sur le pool. Vous pouvez également affecter explicitement des postes de travail à des utilisateurs. Si vous n'activez pas l'affectation automatique, vous devez affecter explicitement un poste de travail à chaque utilisateur.	
vCenter Server	Sélectionnez le serveur vCenter Server qui gère les machines virtuelles dans le pool.	

Tableau 5-1. Feuille de calcul : options de configuration pour créer un pool automatisé contenant des machines virtuelles complètes (suite)

Option	Description	Indiquez votre valeur ici
ID de pool	Nom unique qui identifie le pool dans View Administrator. Si plusieurs serveurs vCenter Server sont exécutés dans votre environnement, assurez-vous qu'aucun autre serveur vCenter Server n'utilise le même ID de pool. Une configuration de Serveur de connexion View peut être une instance de Serveur de connexion View autonome ou un groupe d'instances répliquées qui partagent une configuration View LDAP commune.	
Nom d'affichage	Nom de pool que les utilisateurs voient lorsqu'ils ouvrent une session avec View Client. Si vous ne spécifiez pas de nom d'affichage, l'ID de pool est affiché aux utilisateurs.	
Dossier View	Sélectionnez un dossier View dans lequel placer le pool ou laissez le pool dans le dossier racine par défaut. Si vous utilisez un dossier View, vous pouvez déléguer la gestion du pool à un administrateur avec un rôle spécifique. Pour plus d'informations, reportez-vous à la section « Utilisation de dossiers pour déléguer l'administration », page 42. **Remarque** Les dossiers View sont différents des dossiers vCenter Server qui stockent des machines virtuelles de poste de travail. Vous sélectionnez un dossier vCenter Server plus tard dans l'assistant avec d'autres paramètres de vCenter Server.	
Supprimer le poste de travail après la fermeture de session	Si vous sélectionnez une affectation d'utilisateur flottante, choisissez si vous voulez supprimer des postes de travail quand les utilisateurs ferment leur session. **Remarque** Vous définissez cette option sur la page Paramètres de pool.	
Paramètres de pool	Paramètres qui déterminent l'état du poste de travail, l'état d'alimentation quand une machine virtuelle n'est pas utilisée, le protocole d'affichage, la qualité Adobe Flash, etc. Pour voir des descriptions, reportez-vous à la section « Paramètres de poste de travail et de pool », page 151. Pour voir une liste des paramètres qui s'appliquent à des pools automatisés, reportez-vous à la section « Paramètres de poste de travail pour des pools automatisés contenant des machines virtuelles complètes », page 102. Pour plus d'informations sur les règles d'alimentation et les pools automatisés, reportez-vous à la section « Définition de règles d'alimentation pour des pools de postes de travail », page 161.	

Tableau 5-1. Feuille de calcul : options de configuration pour créer un pool automatisé contenant des machines virtuelles complètes (suite)

Option	Description	Indiquez votre valeur ici
Attribution de nom aux machines virtuelles	Choisissez si vous souhaitez approvisionner des postes de travail en spécifiant manuellement une liste de noms de poste de travail ou en fournissant un mode d'attribution de nom et le nombre total de postes de travail. Pour plus d'informations, reportez-vous à la section « Nommer des postes de travail manuellement ou fournir un mode d'attribution de nom », page 144.	
Liste de noms de poste de travail	Si vous spécifiez des noms manuellement, préparez une liste de noms de poste de travail et, éventuellement, les noms d'utilisateur associés.	
Mode d'attribution de nom	Si vous utilisez cette méthode de nommage, fournissez le mode. View Manager utilise votre mode comme préfixe dans tous les noms de poste de travail et ajoute un numéro unique pour identifier chaque poste de travail. Pour plus d'informations, reportez-vous à la section « Utilisation d'un mode d'attribution de nom pour des pools de postes de travail automatisés », page 147.	
Nombre maximum de postes de travail	Si vous utilisez un mode d'attribution de nom, spécifiez le nombre total de postes de travail dans le pool. Vous pouvez également spécifier un nombre minimum de postes de travail à approvisionner quand vous créez le pool.	
Nombre de postes de travail de rechange (activés)	Si vous spécifiez des noms manuellement ou que vous utilisez un mode d'attribution de nom, spécifiez un nombre de postes de travail que View Manager maintient disponibles et activés pour les nouveaux utilisateurs. Pour plus d'informations, reportez-vous à la section « Nommer des postes de travail manuellement ou fournir un mode d'attribution de nom », page 144. Lorsque vous spécifiez des noms manuellement, cette option est appelée **[# Nb de postes de travail non affectés maintenus activés]** .	
Nombre minimum de postes de travail	Si vous utilisez un mode d'attribution de nom et que vous approvisionnez des postes de travail à la demande, spécifiez un nombre minimum de postes de travail dans le pool. View Manager crée le nombre minimum de postes de travail quand vous créez le pool. Si vous approvisionnez des postes de travail à la demande, View Manager crée dynamiquement des postes de travail supplémentaires à mesure que les utilisateurs se connectent au pool pour la première fois ou à mesure que vous affectez des postes de travail à des utilisateurs.	
Modèle	Sélectionnez le modèle de machine virtuelle que View Manager utilise pour créer le pool.	
Dossier vCenter Server	Sélectionnez le dossier dans vCenter Server dans lequel réside le pool de postes de travail.	

Tableau 5-1. Feuille de calcul : options de configuration pour créer un pool automatisé contenant des machines virtuelles complètes (suite)

Option	Description	Indiquez votre valeur ici
Hôte ou cluster	Sélectionnez l'hôte ou le cluster ESX sur lequel les machines virtuelles de poste de travail s'exécutent. Dans vSphere 5.1 ou supérieur, vous pouvez sélectionner un cluster avec 32 hôtes ESXi maximum.	
Pool de ressources	Sélectionnez le pool de ressources de vCenter Server dans lequel le pool de postes de travail réside.	
Magasins de données	Sélectionnez un ou plusieurs magasins de données sur lesquels stocker le pool de postes de travail. Pour les clusters, vous pouvez utiliser des magasins des données partagés ou locaux.	
Utiliser View Storage Accelerator	Déterminez si les hôtes ESXi mettent en cache des données de disque de machine virtuelle communes. View Storage Accelerator peut améliorer les performances et réduire le besoin de bande passante d'E/S de stockage supplémentaire pour gérer des tempêtes de démarrage et des tempêtes d'E/S d'analyse antivirus. Cette fonction est prise en charge sur vSphere 5.0 et supérieur. Cette fonction est activée par défaut. Pour plus d'informations, reportez-vous à la section « Configurer View Storage Accelerator pour des pools de postes de travail », page 167.	
Personnalisation client	Sélectionnez une spécification de personnalisation (SYSPREP) dans la liste pour permettre à View Manager de configurer des paramètres de licence, d'association de domaine, de protocole DHCP et d'autres propriétés sur les postes de travail. Vous pouvez également personnaliser les postes de travail manuellement quand View Manager les crée.	

Créer un pool automatisé contenant des machines virtuelles complètes

Vous pouvez créer un pool de postes de travail automatisé basé sur un modèle de machine virtuelle que vous sélectionnez. View Manager déploie dynamiquement les postes de travail, en créant une nouvelle machine virtuelle dans vCenter Server pour chaque poste de travail.

Pour créer un pool de clone lié, reportez-vous à la section « Pools de postes de travail de clone lié », page 103.

Prérequis

- Préparez un modèle de machine virtuelle que View Manager utilisera pour créer les postes de travail. View Agent doit être installé sur le modèle. Reportez-vous à la section Chapitre 4, « Création et préparation de machines virtuelles », page 65.
- Si vous prévoyez d'utiliser une spécification de personnalisation, assurez-vous que les spécifications sont exactes. Dans vSphere Client, déployez et personnalisez une machine virtuelle depuis votre modèle à l'aide de la spécification de personnalisation. Testez entièrement la machine virtuelle résultante, notamment DHCP et l'authentification.

- Vérifiez que vous possédez un nombre suffisant de ports sur le commutateur virtuel ESX utilisé pour les machines virtuelles de poste de travail. La valeur par défaut peut ne pas être suffisante si vous créez des pools de postes de travail volumineux. Le nombre de ports de commutateur virtuel sur l'hôte ESX doit être égal ou supérieur au nombre de machines virtuelles de poste de travail multiplié par le nombre de cartes réseau virtuelles par machine virtuelle.
- Collectez les informations de configuration que vous devez fournir pour créer le pool. Reportez-vous à la section « Feuille de calcul pour créer un pool automatisé contenant des machines virtuelles complètes », page 98.
- Décidez comment configurer les paramètres d'alimentation, le protocole d'affichage, la qualité Adobe Flash et d'autres paramètres. Reportez-vous à la section « Paramètres de poste de travail et de pool », page 151.
- Si vous prévoyez de fournir l'accès à vos postes de travail via Horizon Workspace, vérifiez que vous créez les pools de postes de travail en tant qu'utilisateur avec des autorisations Administrateurs dans le dossier racine dans View. Si vous accordez à l'utilisateur des autorisations Administrateurs sur un dossier autre que le dossier racine, Horizon Workspace ne reconnaîtra pas l'authentificateur SAML que vous configurez dans View et vous ne pouvez pas configurer le pool dans Horizon Workspace.

Procédure

1 Dans View Administrator, cliquez sur **[Inventory (Inventaire)] > [Pools]** .

2 Cliquez sur **[Add (Ajouter)]** .

3 Sélectionnez **[Pool automatisé]** .

4 Sur la page vCenter Server, choisissez **[Machines virtuelles complètes]** .

5 Suivez les invites de l'assistant pour créer le pool.

   Utilisez les informations de configuration que vous avez collectées dans la feuille de calcul. Vous pouvez revenir directement à n'importe quelle page de l'assistant en cliquant sur le nom de page dans le volet de navigation.

Dans View Administrator, vous pouvez voir les postes de travail lorsqu'ils sont ajoutés au pool en cliquant sur **[Inventaire] > [Postes de travail]** .

Suivant

Autorisez les utilisateurs à accéder au pool. Reportez-vous à la section « Ajouter des autorisations à des pools de postes de travail », page 171.

Paramètres de poste de travail pour des pools automatisés contenant des machines virtuelles complètes

Vous devez spécifier des paramètres de poste de travail et de pool lorsque vous configurez des pools automatisés contenant des machines virtuelles complètes. Différents paramètres s'appliquent à des pools avec des affectations d'utilisateur dédiées et flottantes.

Tableau 5-2 répertorie les paramètres qui s'appliquent à des pools automatisés avec des affectations dédiées et flottantes.

Pour voir des descriptions de chaque paramètre de poste de travail, reportez-vous à la section « Paramètres de poste de travail et de pool », page 151.

Tableau 5-2. Paramètres des pools automatisés contenant des machines virtuelles complètes

Paramètre	Pool automatisé, affectation dédiée	Pool automatisé, affectation flottante
État	Oui	Oui
Restrictions de Serveur de connexion	Oui	Oui

Tableau 5-2. Paramètres des pools automatisés contenant des machines virtuelles complètes (suite)

Paramètre	Pool automatisé, affectation dédiée	Pool automatisé, affectation flottante
Règle d'alimentation de poste de travail distant	Oui	Oui
Fermeture de session automatique après la déconnexion	Oui	Oui
Autoriser les utilisateurs à réinitialiser leurs postes de travail	Oui	Oui
Autoriser plusieurs sessions par utilisateur		Oui
Supprimer le poste de travail après la fermeture de session		Oui
Protocole d'affichage par défaut	Oui	Oui
Autoriser les utilisateurs à choisir un protocole	Oui	Oui
Convertisseur 3D	Oui	Oui
Nombre max. d'écrans	Oui	Oui
Résolution max. d'un écran	Oui	Oui
Qualité Adobe Flash	Oui	Oui
Limitation d'Adobe Flash	Oui	Oui

Pools de postes de travail de clone lié

Pour créer un pool de postes de travail de clone lié, View Composer génère des machines virtuelles de clone lié depuis un snapshot d'une machine virtuelle parente. View Manager approvisionne dynamiquement les postes de travail de clone lié en fonction des paramètres que vous appliquez au pool.

Comme les postes de travail de clone lié partagent une image du disque système de base, ils utilisent moins de stockage que les machines virtuelles complètes.

Feuille de calcul pour créer un pool de postes de travail de clone lié

Lorsque vous créez un pool de postes de travail de clone lié, l'assistant Ajouter un pool de View Administrator vous invite à configurer certaines options. Utilisez cette feuille de calcul pour préparer vos options de configuration avant de créer le pool.

Vous pouvez imprimer cette feuille de calcul et noter les valeurs que vous souhaitez spécifier quand vous exécutez l'assistant Ajouter un pool.

Avant de créer un pool de clone lié, vous devez utiliser vCenter Server pour prendre un snapshot de la machine virtuelle parente que vous préparez pour le pool. Vous devez éteindre la machine virtuelle parente avant de prendre le snapshot. View Composer utilise le snapshot comme image de base depuis laquelle les clones sont créés.

Remarque Vous ne pouvez pas créer de pool de clone lié depuis un modèle de machine virtuelle.

Tableau 5-3. Feuille de calcul : options de configuration pour créer un pool de postes de travail de clone lié

Option	Description	Indiquez votre valeur ici
Affectation d'utilisateur	Choisissez le type d'affectation d'utilisateur : ■ Dans un pool d'affectation dédiée, chaque utilisateur est affecté à un poste de travail. Les utilisateurs reçoivent le même poste de travail chaque fois qu'ils ouvrent une session. ■ Dans un pool d'affectation flottante, les utilisateurs reçoivent différents postes de travail chaque fois qu'ils ouvrent une session. Pour plus d'informations, reportez-vous à la section « Affectation d'utilisateur dans des pools de postes de travail », page 143.	
Activer l'affectation automatique	Dans un pool d'affectation dédiée, un poste de travail est affecté à un utilisateur quand l'utilisateur ouvre d'abord une session sur le pool. Vous pouvez également affecter explicitement des postes de travail à des utilisateurs. Si vous n'activez pas l'affectation automatique, vous devez affecter explicitement un poste de travail à chaque utilisateur.	
vCenter Server	Sélectionnez le serveur vCenter Server qui gère les machines virtuelles dans le pool.	
ID de pool	Nom unique qui identifie le pool dans View Administrator. Si plusieurs configurations de Serveur de connexion View sont exécutées dans votre environnement, assurez-vous qu'aucune autre configuration de Serveur de connexion View n'utilise le même ID de pool. Une configuration de Serveur de connexion View peut être une instance de Serveur de connexion View autonome ou un groupe d'instances répliquées qui partagent une configuration View LDAP commune.	
Nom d'affichage	Nom de pool que les utilisateurs voient lorsqu'ils ouvrent une session avec View Client. Si vous ne spécifiez pas de nom d'affichage, l'ID de pool est affiché aux utilisateurs.	
Dossier View	Sélectionnez un dossier View dans lequel placer le pool ou laissez le pool dans le dossier racine par défaut. Si vous utilisez un dossier View, vous pouvez déléguer la gestion du pool à un administrateur avec un rôle spécifique. Pour plus d'informations, reportez-vous à la section « Utilisation de dossiers pour déléguer l'administration », page 42. **Remarque** Les dossiers View sont différents des dossiers vCenter Server qui stockent des machines virtuelles de poste de travail. Vous sélectionnez un dossier vCenter Server plus tard dans l'assistant avec d'autres paramètres de vCenter Server.	
Supprimer ou actualiser le poste de travail à la fermeture de session	Si vous sélectionnez une affectation d'utilisateur flottante, choisissez si vous voulez actualiser des postes de travail, les supprimer ou ne rien faire quand les utilisateurs ferment leur session. **Remarque** Vous définissez cette option sur la page Paramètres de pool.	

Tableau 5-3. Feuille de calcul : options de configuration pour créer un pool de postes de travail de clone lié (suite)

Option	Description	Indiquez votre valeur ici
Paramètres de pool	Paramètres qui déterminent l'état du poste de travail, l'état d'alimentation quand une machine virtuelle n'est pas utilisée, le protocole d'affichage, la qualité Adobe Flash, etc. Pour voir des descriptions, reportez-vous à la section « Paramètres de poste de travail et de pool », page 151. Pour voir une liste des paramètres qui s'appliquent à des pools de clone lié, reportez-vous à la section « Paramètres de poste de travail pour des pools de postes de travail de clone lié », page 115. Pour plus d'informations sur les règles d'alimentation et les pools automatisés, reportez-vous à la section « Définition de règles d'alimentation pour des pools de postes de travail », page 161.	
Attribution de nom aux machines virtuelles	Choisissez si vous souhaitez approvisionner des postes de travail en spécifiant manuellement une liste de noms de poste de travail ou en fournissant un mode d'attribution de nom et le nombre total de postes de travail. Pour plus d'informations, reportez-vous à la section « Nommer des postes de travail manuellement ou fournir un mode d'attribution de nom », page 144.	
Liste de noms de poste de travail	Si vous spécifiez des noms manuellement, préparez une liste de noms de poste de travail et, éventuellement, les noms d'utilisateur associés.	
Mode d'attribution de nom	Si vous utilisez cette méthode de nommage, fournissez le mode. View Manager utilise votre mode comme préfixe dans tous les noms de poste de travail et ajoute un numéro unique pour identifier chaque poste de travail. Pour plus d'informations, reportez-vous à la section « Utilisation d'un mode d'attribution de nom pour des pools de postes de travail automatisés », page 147.	
Nombre max. de postes de travail	Si vous utilisez un mode d'attribution de nom, spécifiez le nombre total de postes de travail dans le pool. Vous pouvez également spécifier un nombre minimum de postes de travail à approvisionner quand vous créez le pool.	
Nombre de postes de travail de rechange (activés)	Si vous spécifiez des noms manuellement ou que vous utilisez un mode d'attribution de nom, spécifiez un nombre de postes de travail que View Manager maintient disponibles et activés pour les nouveaux utilisateurs. Pour plus d'informations, reportez-vous à la section « Nommer des postes de travail manuellement ou fournir un mode d'attribution de nom », page 144. Lorsque vous spécifiez des noms manuellement, cette option est appelée **[# Nb de postes de travail non affectés maintenus activés]** .	

Tableau 5-3. Feuille de calcul : options de configuration pour créer un pool de postes de travail de clone lié (suite)

Option	Description	Indiquez votre valeur ici
Minimum number of ready (provisioned) desktops during Nombre minimal de postes de travail prêts (approvisionnés) lors d'opérations de maintenance de View Composer	Si vous spécifiez des noms manuellement ou si vous utilisez un mode d'attribution de nom, spécifiez un nombre minimal de postes de travail qui sont prêts et approvisionnés lorsque des opérations de View Composer sont en cours. Ce paramètre vous permet de maintenir les postes de travail approvisionnés et prêts à accepter les demandes de connexion d'utilisateurs lorsque View Composer actualise, recompose ou rééquilibre les postes de travail dans le pool. Cette valeur doit être inférieure à la valeur **[Nombre min. de postes de travail]** , que vous spécifiez si vous approvisionnez des postes de travail à la demande. Reportez-vous à la section « Maintien des postes de travail de clone lié approvisionnés et prêts lors d'opérations de View Composer », page 133.	
Approvisionner des postes de travail à la demande ou Approvisionner tous les postes de travail à l'avance	Si vous utilisez un mode d'attribution de nom, choisissez d'approvisionner tous les postes de travail lorsque le pool est créé ou d'approvisionner les postes de travail à mesure qu'ils sont nécessaires. ■ **[Approvisionner tous les postes de travail à l'avance]** . Lorsque le pool est créé, View Manager approvisionne le nombre de postes de travail que vous spécifiez dans **[Nombre max. de postes de travail]** . ■ **[Approvisionner des postes de travail à la demande]** . Lorsque le pool est créé, View Manager crée le nombre de postes de travail que vous spécifiez dans **[Nombre min. de postes de travail]** . View Manager crée dynamiquement des postes de travail supplémentaires à mesure que les utilisateurs se connectent au pool pour la première fois ou à mesure que vous affectez des postes de travail à des utilisateurs.	
Nombre min. de postes de travail	Si vous utilisez un mode d'attribution de nom et que vous approvisionnez des postes de travail à la demande, spécifiez un nombre minimum de postes de travail dans le pool. View Manager crée le nombre minimum de postes de travail quand vous créez le pool. View Manager conserve le nombre minimal de postes de travail même lorsque d'autres paramètres tels que **[Supprimer ou actualiser le poste de travail à la fermeture de session]** entraînent la suppression des postes de travail.	

Tableau 5-3. Feuille de calcul : options de configuration pour créer un pool de postes de travail de clone lié (suite)

Option	Description	Indiquez votre valeur ici
Rediriger un profil Windows vers des disques persistants	Si vous sélectionnez des affectations d'utilisateur dédiées, choisissez si vous voulez stocker des données de profil d'utilisateur Windows sur un disque persistant séparé de View Composer ou sur le même disque que les données du système d'exploitation. Les disques persistants séparés vous permettent de conserver des données et des paramètres d'utilisateur. Les opérations d'actualisation, de recomposition et de rééquilibrage de View Composer n'affectent pas les disques persistants. Vous pouvez détacher un disque persistant d'un clone lié et recréer le poste de travail de clone lié à partir du disque détaché. Par exemple, lorsqu'un poste de travail ou un pool est supprimé, vous pouvez détacher le disque persistant et recréer le poste de travail, en conservant les données et les paramètres d'utilisateur d'origine. Si vous stockez le profil Windows sur le disque du système d'exploitation, les données et les paramètres d'utilisateur sont supprimés au cours des opérations d'actualisation, de recomposition et de rééquilibrage.	
Taille et lettre des disques persistants	Si vous stockez des données de profil d'utilisateur sur un disque persistant séparé de View Composer, fournissez la taille du disque en mégaoctets et la lettre du lecteur. **Remarque** Ne sélectionnez pas de lettre de lecteur qui existe déjà sur la machine virtuelle parente ou qui entre en conflit avec une lettre de lecteur utilisée pour un lecteur monté en réseau.	
Redirection de fichier supprimable	Choisissez si vous voulez rediriger les fichiers d'échange et temporaires du système d'exploitation client sur un disque non persistant séparé. Si vous le faites, fournissez la taille de disque en mégaoctets. Avec cette configuration, lorsqu'un clone lié est mis hors tension, View Manager remplace le disque de fichier supprimable par une copie du disque d'origine créé avec le pool de clone lié. La taille des clones liés peut augmenter à mesure que les utilisateurs interagissent avec leurs postes de travail. La redirection du fichier supprimable peut économiser de l'espace de stockage en ralentissant la croissance des clones liés.	

Tableau 5-3. Feuille de calcul : options de configuration pour créer un pool de postes de travail de clone lié (suite)

Option	Description	Indiquez votre valeur ici
Taille et lettre des disques de fichier supprimables	Si vous redirigez des fichiers supprimables vers un disque non persistant, fournissez la taille du disque en mégaoctets et la lettre du lecteur. La taille de disque doit être supérieure à la taille du fichier d'échange du système d'exploitation client. Pour déterminer la taille du fichier d'échange, reportez-vous à la section « Conserver une trace de la taille du fichier d'échange de la machine virtuelle parente », page 94. Lorsque vous configurez la taille du disque de fichier supprimable, prenez bien en considération que la taille réelle d'une partition de disque formaté est légèrement plus petite que la valeur que vous fournissez dans View Administrator. Vous pouvez sélectionner une lettre de lecteur pour le disque de fichier supprimable. La valeur par défaut, **[Auto]** , demande à View d'affecter la lettre de lecteur. **Remarque** Ne sélectionnez pas de lettre de lecteur qui existe déjà sur la machine virtuelle parente ou qui entre en conflit avec une lettre de lecteur utilisée pour un lecteur monté en réseau.	
Sélectionner des magasins de données séparés pour des disques persistants et du système d'exploitation	Si vous redirigez des profils d'utilisateur vers des disques persistants séparés, vous pouvez stocker les disques persistants et les disques du système d'exploitation sur des magasins de données différents.	
Sélectionner des magasins de données séparés pour des disques de réplica et du système d'exploitation	Vous pouvez stocker le disque de machine virtuelle réplica (maître) sur un magasin de données haute performance et les clones liés sur des magasins de données séparés. Pour plus d'informations, reportez-vous à la section « Stockage de réplicas et de clones liés View Composer sur des magasins de données séparés », page 128. Si vous stockez des réplicas et des disques du système d'exploitation sur des magasins de données séparés, des snapshots NFS natifs ne peuvent pas être utilisés. Le clonage natif sur un périphérique NAS ne peut avoir lieu que si les disques de réplica et du système d'exploitation sont stockés sur les mêmes magasins de données.	
Machine virtuelle parente	Sélectionnez la machine virtuelle parente du pool. Pour utiliser des fonctions prises en charge dans View Manager 4.5 ou supérieur, telles que la redirection de données supprimables sur un disque séparé et la personnalisation des clones liés avec Sysprep, vous devez sélectionner une machine virtuelle parente sur laquelle View Agent 4.5 ou supérieur est installé. **Remarque** Vous ne pouvez pas utiliser View Composer pour déployer des postes de travail qui exécutent Windows Vista Ultimate Edition ou Windows XP Professional SP1.	

Tableau 5-3. Feuille de calcul : options de configuration pour créer un pool de postes de travail de clone lié (suite)

Option	Description	Indiquez votre valeur ici
Image par défaut (snapshot)	Sélectionnez le snapshot de la machine virtuelle parente à utiliser comme image de base pour le pool. Ne supprimez pas le snapshot et la machine virtuelle parente de vCenter Server, sauf si aucun clone lié dans le pool n'utilise l'image par défaut, et si aucun autre clone lié ne sera créé à partir de cette image par défaut. View Manager requiert la machine virtuelle parente et le snapshot pour approvisionner de nouveaux clones liés dans le pool, conformément aux règles de pool. La machine virtuelle parente et le snapshot sont également requis pour les opérations de maintenance de View Composer.	
Publiez une image de base pour le référentiel de Serveur de transfert.	Sélectionnez cette option si vous utilisez le pool pour approvisionner des postes de travail locaux. Lorsqu'un poste de travail local est approvisionné, Serveur de transfert View télécharge l'image de base depuis le référentiel de Serveur de transfert sur le client. Vous pouvez également publier l'image de base après avoir créé le pool.	
Dossier vCenter Server	Sélectionnez le dossier dans vCenter Server dans lequel réside le pool de postes de travail.	
Hôte ou cluster	Sélectionnez l'hôte ou le cluster ESX sur lequel les machines virtuelles de poste de travail s'exécutent. Dans vSphere 5.1 ou supérieur, vous pouvez sélectionner un cluster contenant jusqu'à 32 hôtes ESXi si les réplicas sont stockés sur des magasins de données VMFS5 ou supérieur ou sur des magasins de données NFS. Si vous stockez les réplicas sur une version VMFS antérieure à VMFS5, un cluster peut contenir 8 hôtes au maximum. Dans vSphere 5.0, vous pouvez sélectionner un cluster avec plus de 8 hôtes ESXi si les réplicas sont stockés sur des magasins de données NFS. Si vous stockez les réplicas sur des magasins de données VMFS, un cluster peut contenir au maximum 8 hôtes. Reportez-vous à la section « Configuration de pools sur des clusters avec plus de huit hôtes », page 169.	
Pool de ressources	Sélectionnez le pool de ressources de vCenter Server dans lequel le pool de postes de travail réside.	

Tableau 5-3. Feuille de calcul : options de configuration pour créer un pool de postes de travail de clone lié (suite)

Option	Description	Indiquez votre valeur ici
Sélectionner des magasins de données	Sélectionnez un ou plusieurs magasins de données sur lesquels stocker le pool de postes de travail. Un tableau sur la page **[Sélectionner des magasins de données]** de l'assistant Ajouter un pool offre des recommandations très utiles pour l'estimation des exigences de stockage du pool. Ces recommandations peuvent vous aider à déterminer les magasins de données assez volumineux pour stocker les disques de clone lié. Pour plus d'informations, reportez-vous à la section « Dimensionnement du stockage pour des pools de postes de travail de clone lié », page 121. Vous pouvez utiliser des magasins de données partagés ou locaux pour un hôte ESXi individuel ou pour des clusters ESXi. Si vous utilisez des magasins de données locaux dans un cluster ESXi, vous devez prendre en compte les contraintes de l'infrastructure vSphere qui sont imposées sur votre déploiement de poste de travail. Reportez-vous à la section « Stockage des postes de travail de clone liés dans des magasins de données locaux », page 127. Dans vSphere 5.1 ou supérieur, un cluster peut contenir plus de huit hôtes ESXi si les réplicas sont stockés sur des magasins de données VMFS5 ou supérieur ou NFS. Dans vSphere 5.0, un cluster peut contenir plus de huit hôtes ESXi uniquement si les réplicas sont stockés sur des magasins de données NFS. Reportez-vous à la section « Configuration de pools sur des clusters avec plus de huit hôtes », page 169. Pour plus d'informations sur les disques créés pour des clones liés, reportez-vous à la section « Disques de données du poste de travail de clone lié », page 135.	
Surcharge du stockage	Déterminez le niveau de surcharge du stockage auquel View Manager crée des postes de travail de clone lié sur chaque magasin de données. À mesure que le niveau augmente, plus de clones liés sont placés sur le magasin de données et moins d'espace est réservé pour la croissance des clones individuels. Un niveau de surcharge du stockage élevé vous permet de créer des clones liés ayant une taille logique totale supérieure à la limite de stockage physique du magasin de données. Pour plus d'informations, reportez-vous à la section « Définir le niveau de surcharge de stockage pour des postes de travail de clone lié », page 125.	

Tableau 5-3. Feuille de calcul : options de configuration pour créer un pool de postes de travail de clone lié (suite)

Option	Description	Indiquez votre valeur ici
Utiliser View Storage Accelerator	Déterminez si vous voulez utiliser View Storage Accelerator, ce qui permet aux hôtes ESXi de mettre en cache des données de disque de machine virtuelle communes. View Storage Accelerator peut améliorer les performances et réduire le besoin de bande passante d'E/S de stockage supplémentaire pour gérer des tempêtes de démarrage et des tempêtes d'E/S d'analyse antivirus. Cette fonction est prise en charge sur vSphere 5.0 et supérieur. Cette fonction est activée par défaut. Pour plus d'informations, reportez-vous à la section « Configurer View Storage Accelerator pour des pools de postes de travail », page 167.	
Utiliser des snapshots NFS natifs (VAAI) - Présentation technique	Si votre déploiement inclut des périphériques NAS prenant en charge VAAI (vStorage APIs for Array Integration), vous pouvez utiliser la technologie de snapshot natif pour cloner des machines virtuelles. **Remarque** La technologie de snapshot NFS natif (VAAI) est une fonction de la présentation technique. La fonction est disponible à l'essai, mais il n'est pas conseillé de l'utiliser en production et aucun support n'est fourni. Vous pouvez utiliser cette fonction uniquement si vous sélectionnez des magasins de données résidant sur des périphériques NAS prenant en charge les opérations de clonage natif via VAAI. Vous ne pouvez pas utiliser cette fonction si vous stockez des réplicas et des disques du système d'exploitation sur des magasins de données séparés. Vous ne pouvez pas utiliser cette fonction dans un pool activé pour View Storage Accelerator ou pour la récupération d'espace disque de machine virtuelle. Cette fonction est prise en charge sur vSphere 5.0 et supérieur. Pour plus d'informations, reportez-vous à la section « Utilisation de View Composer Array Integration avec la technologie de snapshot NFS natif (VAAI) », page 129.	
Récupérer l'espace disque de machine virtuelle	Déterminez si vous voulez autoriser les hôtes ESXi à récupérer l'espace disque inutilisé sur les clones liés qui sont créés au format de disque à optimisation d'espace. La fonction de récupération d'espace réduit l'espace de stockage total requis pour les postes de travail de clone lié. Cette fonction est prise en charge sur vSphere 5,1 et supérieur. Les machines virtuelles de clone lié doivent avoir la version matérielle virtuelle 9 ou supérieure. Pour plus d'informations, reportez-vous à la section « Récupérer de l'espace disque sur des postes de travail de clone lié », page 130.	

Tableau 5-3. Feuille de calcul : options de configuration pour créer un pool de postes de travail de clone lié (suite)

Option	Description	Indiquez votre valeur ici
Initier la récupération lorsque l'espace inutilisé de la machine virtuelle dépasse :	Tapez la quantité minimale d'espace disque inutilisé, en gigaoctets, qui doit être atteinte sur un disque du système d'exploitation de clone lié pour déclencher la récupération d'espace. Lorsque l'espace disque inutilisé dépasse ce seuil, View initie l'opération qui demande à l'hôte ESXi de récupérer l'espace sur le disque du système d'exploitation. Cette valeur est mesurée par machine virtuelle. L'espace disque inutilisé doit dépasser le seuil spécifié sur une machine virtuelle individuelle pour que View démarre le processus de récupération d'espace sur cette machine. Par exemple : **2** Go. La valeur par défaut est 1 Go.	
Durée d'interruption	Configurez les jours et les heures auxquels la régénération View Storage Accelerator et la récupération de l'espace disque de machine virtuelle n'ont pas lieu. Pour vous assurer que des ressources ESXi sont dédiées à des tâches de premier plan lorsque cela est nécessaire, vous pouvez empêcher les hôtes ESXi d'exécuter ces opérations pendant des périodes de temps spécifiées certains jours. Pour plus d'informations, reportez-vous à la section « Définir des heures d'interruption pour des opérations ESXi sur des postes de travail View », page 132.	
Domaine Active Directory	Sélectionnez le domaine Active Directory et le nom d'utilisateur. View Composer requiert certains privilèges d'utilisateur pour créer un pool de clone lié. Le domaine et le compte d'utilisateur sont utilisés par QuickPrep ou Sysprep pour personnaliser les postes de travail de clone lié. Pour plus d'informations, reportez-vous à la section « Créer un compte d'utilisateur pour View Composer », page 15. Vous spécifiez cet utilisateur lorsque vous configurez des paramètres de View Composer pour vCenter Server. Pour plus d'informations, reportez-vous à la section « Configurer les paramètres de View Composer », page 18. Vous pouvez spécifier plusieurs domaines et utilisateurs lorsque vous configurez les paramètres de View Composer. Lorsque vous utilisez l'assistant Ajouter un pool pour créer un pool, vous devez sélectionner un domaine et un utilisateur dans la liste.	
Conteneur Active Directory	Fournissez le nom unique relatif du conteneur Active Directory. Par exemple : **`CN=Computers`** Lorsque vous exécutez l'assistant Ajouter un pool, vous pouvez parcourir votre arborescence Active Directory pour rechercher le conteneur.	

Tableau 5-3. Feuille de calcul : options de configuration pour créer un pool de postes de travail de clone lié (suite)

Option	Description	Indiquez votre valeur ici
Utiliser QuickPrep ou une spécification de personnalisation (Sysprep)	Choisissez si vous voulez utiliser QuickPrep ou sélectionner une spécification de personnalisation (Sysprep) pour laisser View Manager configurer des paramètres de licence, d'association de domaine, de protocole DHCP et d'autres propriétés sur les postes de travail. Sysprep est pris en charge pour les clones liés uniquement sur le logiciel vSphere 4.1 ou supérieur. Une fois que vous utilisez QuickPrep ou Sysprep lorsque vous créez un pool, vous ne pouvez pas passer à une autre méthode de personnalisation, lorsque vous créez ou recomposez des postes de travail dans le pool. Pour plus d'informations, reportez-vous à la section « Choisir QuickPrep ou Sysprep pour personnaliser des postes de travail de clone lié », page 117.	
Script de désactivation	QuickPrep peut exécuter un script de personnalisation sur des postes de travail de clone lié avant leur désactivation. Fournissez le chemin d'accès vers le script sur la machine virtuelle parente.	
Script de post-synchronisation	QuickPrep peut exécuter un script de personnalisation sur des postes de travail de clone lié après leur création, leur recomposition et leur actualisation. Fournissez le chemin d'accès vers le script sur la machine virtuelle parente.	
Autoriser la réutilisation de comptes d'ordinateur pré-existants	Sélectionnez cette option pour utiliser des comptes d'ordinateur existants dans Active Directory pour des clones liés qui sont approvisionnés par View Composer. Cette option vous permet de contrôler les comptes d'ordinateur qui sont créés dans Active Directory. Lorsqu'un clone lié est approvisionné, si un nom de compte d'ordinateur AD existant correspond au nom du poste de travail de clone lié, View Composer utilise le compte d'ordinateur existant. Sinon, un nouveau compte d'ordinateur est créé. Les comptes d'ordinateur existants doivent être situés dans le conteneur Active Directory que vous spécifiez avec le paramètre **[Conteneur Active Directory]** . Lorsque cette option est désactivée, un nouveau compte d'ordinateur AD est créé lorsque View Composer approvisionne un clone lié. Par défaut, cette option est désactivée. Pour plus d'informations, reportez-vous à la section « Utiliser des comptes d'ordinateur Active Directory existants pour des clones liés », page 133.	

Créer un pool de postes de travail de clone lié

Vous pouvez créer un pool de postes de travail de clone lié automatisé basé sur une machine virtuelle parente que vous sélectionnez. Le service View Composer crée dynamiquement une nouvelle machine virtuelle de clone lié dans vCenter Server pour chaque poste de travail.

Pour créer un pool automatisé contenant des machines virtuelles complètes, reportez-vous à la section « Pools automatisés contenant des machines virtuelles complètes », page 98.

Prérequis

- Vérifiez que le service View Composer est installé, sur le même hôte que vCenter Server ou sur un hôte séparé, et qu'une base de données View Composer est configurée. Consultez le document *Installation de VMware Horizon View*.
- Vérifiez que les paramètres de View Composer pour vCenter Server sont configurés dans View Administrator. Reportez-vous à la section « Configurer les paramètres de View Composer », page 18.
- Vérifiez que vous possédez un nombre suffisant de ports sur le commutateur virtuel ESX utilisé pour les machines virtuelles de poste de travail. La valeur par défaut peut ne pas être suffisante si vous créez des pools de postes de travail volumineux. Le nombre de ports de commutateur virtuel sur l'hôte ESX doit être égal ou supérieur au nombre de machines virtuelles de poste de travail multiplié par le nombre de cartes réseau virtuelles par machine virtuelle.
- Vérifiez que vous avez préparé une machine virtuelle parente. View Agent doit être installé sur la machine virtuelle parente. Reportez-vous à la section Chapitre 4, « Création et préparation de machines virtuelles », page 65.
- Prenez un snapshot de la machine virtuelle parente dans vCenter Server. Vous devez éteindre la machine virtuelle parente avant de prendre le snapshot. View Composer utilise le snapshot comme image de base depuis laquelle les clones sont créés.

  Remarque Vous ne pouvez pas créer de pool de clone lié depuis un modèle de machine virtuelle.

- Collectez les informations de configuration que vous devez fournir pour créer le pool. Reportez-vous à la section « Feuille de calcul pour créer un pool de postes de travail de clone lié », page 103.
- Décidez comment configurer les paramètres d'alimentation, le protocole d'affichage, la qualité Adobe Flash et d'autres paramètres. Reportez-vous à la section « Paramètres de poste de travail et de pool », page 151.
- Si vous prévoyez de fournir l'accès à vos postes de travail via Horizon Workspace, vérifiez que vous créez les pools de postes de travail en tant qu'utilisateur avec des autorisations Administrateurs dans le dossier racine dans View. Si vous accordez à l'utilisateur des autorisations Administrateurs sur un dossier autre que le dossier racine, Horizon Workspace ne reconnaîtra pas l'authentificateur SAML que vous configurez dans View et vous ne pouvez pas configurer le pool dans Horizon Workspace.

Important Lors de la création d'un pool de clone lié, ne modifiez pas la machine virtuelle parente dans vCenter Server. Par exemple, ne convertissez pas la machine virtuelle parente en modèle. Le service View Composer requiert que la machine virtuelle parente reste dans un état statique et inchangé lors de la création du pool.

Procédure

1 Dans View Administrator, cliquez sur **[Inventaire] > [Pools]** .

2 Cliquez sur **[Ajouter]** .

3 Sélectionnez **[Pool automatisé]** .

4 Sur la page vCenter Server, choisissez **[Clones liés View Composer]** .

5 Suivez les invites de l'assistant pour créer le pool.

Utilisez les informations de configuration que vous avez collectées dans la feuille de calcul. Vous pouvez revenir directement à n'importe quelle page de l'assistant en cliquant sur le nom de page dans le volet de navigation.

Sur la page **[Paramètres de vCenter]** , vous devez cliquer sur **[Parcourir]** et sélectionner les paramètres de vCenter Server en séquence. Vous ne pouvez pas ignorer un paramètre de vCenter Server :

a Machine virtuelle parente

b Snapshot

c Emplacement du dossier de machine virtuelle

d Hôte ou cluster

e Pool de ressources

f Magasins de données

Dans View Administrator, vous pouvez voir les postes de travail lorsqu'ils sont ajoutés au pool en cliquant sur **[Inventaire] > [Postes de travail]** .

Les clones liés peuvent redémarrer une ou plusieurs fois lors de leur approvisionnement. Si un clone lié est dans un état d'erreur, le mécanisme de récupération automatique de View tente d'activer, ou d'arrêter et de redémarrer, le clone lié. Si des tentatives de récupération répétées échouent, le clone lié est supprimé.

View Composer crée également une machine virtuelle réplica qui sert d'image maître pour l'approvisionnement des clones liés. Pour réduire la consommation d'espace, le réplica est créé en tant que disque fin. Si tous les postes de travail sont recomposés ou supprimés, et qu'aucun clone n'est lié au réplica, la machine virtuelle réplica est supprimée de vCenter Server.

Si vous ne stockez pas le réplica sur un magasin de données séparé, View Composer crée un réplica sur chaque magasin de données sur lequel des clones liés sont créés.

Si vous stockez le réplica sur un magasin de données séparé, un réplica est créé pour le pool entier, même lorsque des clones liés sont créés sur plusieurs magasins de données.

Suivant

Autorisez les utilisateurs à accéder au pool. Reportez-vous à la section « Ajouter des autorisations à des pools de postes de travail », page 171.

Paramètres de poste de travail pour des pools de postes de travail de clone lié

Vous devez spécifier des paramètres de poste de travail et de pool lorsque vous configurez des pools automatisés contenant des postes de travail de clone lié créés par View Composer. Différents paramètres s'appliquent à des pools avec des affectations d'utilisateur dédiées et flottantes.

Tableau 5-4 répertorie les paramètres qui s'appliquent à des pools de clone lié avec des affectations dédiées et flottantes.

Pour voir des descriptions de chaque paramètre de poste de travail, reportez-vous à la section « Paramètres de poste de travail et de pool », page 151.

Tableau 5-4. Paramètres de pools de postes de travail de clone lié automatisés

Paramètre	Pool de clone lié, affectation dédiée	Pool de clone lié, affectation flottante
État	Oui	Oui
Restrictions de Serveur de connexion	Oui	Oui
Règle d'alimentation de poste de travail distant	Oui	Oui

Tableau 5-4. Paramètres de pools de postes de travail de clone lié automatisés (suite)

Paramètre	Pool de clone lié, affectation dédiée	Pool de clone lié, affectation flottante
Fermeture de session automatique après la déconnexion	Oui	Oui
Autoriser les utilisateurs à réinitialiser leurs postes de travail	Oui	Oui
Autoriser plusieurs sessions par utilisateur		Oui
Supprimer ou actualiser le poste de travail à la fermeture de session		Oui
Actualiser le disque du système d'exploitation après la fermeture de session	Oui	
Protocole d'affichage par défaut	Oui	Oui
Autoriser les utilisateurs à choisir un protocole	Oui	Oui
Convertisseur 3D	Oui	Oui
Nombre max. d'écrans	Oui	Oui
Résolution max. d'un écran	Oui	Oui
Qualité Adobe Flash	Oui	Oui
Limitation d'Adobe Flash	Oui	Oui

Prise en charge de View Composer pour les SID de clone lié et les applications tierces

View Composer peut générer et conserver des ID de sécurité (SID) d'ordinateur local pour des machines virtuelles de clone lié dans certaines situations. View Composer peut conserver des identificateurs globaux uniques (GUID) d'applications tierces, en fonction de la façon dont les applications génèrent des GUID.

Pour comprendre comment les opérations de View Composer affectent les SID et les GUID d'application, vous devez comprendre comment les postes de travail de clone lié sont créés et approvisionnés :

1 View Composer crée un clone lié en effectuant ces actions :

   a Il crée le réplica en clonant le snapshot de machine virtuelle parente.

   b Il crée le clone lié pour faire référence au réplica comme son disque parent.

2 View Composer et View Manager personnalisent le clone lié avec QuickPrep ou une spécification de personnalisation Sysprep, en fonction de l'outil de personnalisation que vous sélectionnez lorsque vous créez le pool.

   - Si vous utilisez Sysprep, un SID unique est généré pour chaque clone.
   - Si vous utilisez QuickPrep, aucun nouveau SID n'est généré. Le SID de la machine virtuelle parente est répliqué sur tous les postes de travail de clone lié approvisionnés dans le pool.
   - Certaines applications génèrent un GUID au cours de la personnalisation.

3 View Manager crée un snapshot du clone lié.

   Le snapshot contient le SID unique généré avec Sysprep ou un SID commun généré avec QuickPrep.

4 View Manager active le poste de travail en fonction des paramètres que vous sélectionnez lorsque vous créez le pool.

   Certaines applications génèrent un GUID lors de la première activation du poste de travail.

Pour voir une comparaison des personnalisations QuickPrep et Sysprep, reportez-vous à la section « Choisir QuickPrep ou Sysprep pour personnaliser des postes de travail de clone lié », page 117.

Lorsque vous actualisez le clone lié, View Composer utilise le snapshot pour restaurer le clone à son état initial. Son SID est conservé.

Si vous utilisez QuickPrep, lorsque vous recomposez le clone lié, le SID de la machine virtuelle parente est conservé sur le clone lié tant que vous sélectionnez la même machine virtuelle parente pour l'opération de recomposition. Si vous sélectionnez une machine virtuelle parente différente pour la recomposition, le SID du nouveau parent est répliqué sur le clone.

Si vous utilisez Sysprep, un nouveau SID est toujours généré sur le clone. Pour plus d'informations, reportez-vous à la section « Recomposition de clones liés personnalisés avec Sysprep », page 120.

Tableau 5-5 montre l'effet des opérations de View Composer sur les SID de clones liés et les GUID d'applications tierces.

Tableau 5-5. Opérations de View Composer, SID de clone lié et GUID d'application

Prise en charge de SID ou de GUID	Création de clone	Actualisation	Recomposition
Sysprep : SID uniques pour clones liés	Avec la personnalisation Sysprep, des SID uniques sont générés pour des clones liés.	Les SID uniques sont conservés.	Les SID uniques ne sont pas conservés.
QuickPrep : SID communs pour clones liés	Avec la personnalisation QuickPrep, un SID commun est généré pour tous les clones d'un pool.	Le SID commun est conservé.	Le SID commun est conservé.
GUID d'application tierce	Chaque application se comporte différemment. REMARQUE Sysprep et QuickPrep ont le même effet sur la conservation de GUID.	Le GUID est conservé si une application génère le GUID avant la prise du snapshot initial. Le GUID n'est pas conservé si une application génère le GUID après la prise du snapshot initial.	Les opérations de recomposition ne conservent pas de GUID d'application sauf si l'application inscrit le GUID sur le lecteur spécifié en tant que disque persistant de View Composer.

Choisir QuickPrep ou Sysprep pour personnaliser des postes de travail de clone lié

QuickPrep et Microsoft Sysprep fournissent différentes approches pour personnaliser des postes de travail de clone lié. QuickPrep est conçu pour fonctionner efficacement avec View Composer. Microsoft Sysprep offre des outils de personnalisation standard.

Lorsque vous créez des postes de travail de clone lié, vous devez modifier chaque machine virtuelle pour qu'elle puisse fonctionner en tant qu'ordinateur unique sur le réseau. View Manager et View Composer fournissent deux méthodes pour personnaliser des postes de travail de clone lié.

Tableau 5-6 compare QuickPrep avec des spécifications de personnalisation créées avec Microsoft Sysprep.

Sysprep est pris en charge pour les clones liés uniquement sur le logiciel vSphere 4.1 ou supérieur. Vous ne pouvez pas utiliser Sysprep pour personnaliser des postes de travail de clone lié sur le logiciel vSphere 4.0.

Tableau 5-6. Comparaison de QuickPrep et Microsoft Sysprep

QuickPrep	Spécification de personnalisation (Sysprep)
Conçu pour fonctionner avec View Composer. Pour plus d'informations, reportez-vous à la section « Personnalisation de postes de travail de clone lié avec QuickPrep », page 118.	Peut être créée avec les outils Microsoft Sysprep standard.
Utilise le même ID de sécurité (SID) de l'ordinateur local pour tous les clones liés du pool.	Génère un SID d'ordinateur local unique pour chaque clone lié du pool.
Peut exécuter des scripts de personnalisation supplémentaires avant la désactivation de clones liés et après la création, l'actualisation ou la recomposition de clones liés.	Peut exécuter un script supplémentaire après la première ouverture de session de l'utilisateur.
Associe l'ordinateur de clone lié au domaine Active Directory.	Associe l'ordinateur de clone lié au domaine Active Directory. Les informations de domaine et d'administrateur dans la spécification de personnalisation Sysprep ne sont pas utilisées. La machine virtuelle est associée au domaine à l'aide des informations de personnalisation client que vous entrez dans View Administrator lorsque vous créez le pool.
Pour chaque clone lié, ajoute un ID unique au compte de domaine Active Directory.	Pour chaque clone lié, ajoute un ID unique au compte de domaine Active Directory.
Ne génère pas de nouveau SID après l'actualisation des clones liés. Le SID commun est conservé.	Génère un nouveau SID lors de la personnalisation de chaque clone lié. Conserve les SID uniques au cours d'une opération d'actualisation, mais pas au cours d'une opération de recomposition ou de rééquilibrage.
Ne génère pas de nouveau SID après la recomposition des clones liés. Le SID commun est conservé.	S'exécute de nouveau après la recomposition des clones liés, en générant de nouveaux SID pour les machines virtuelles. Pour plus d'informations, reportez-vous à la section « Recomposition de clones liés personnalisés avec Sysprep », page 120.
S'exécute plus rapidement que Sysprep.	Peut prendre plus de temps que QuickPrep.

Après avoir personnalisé un pool de clone lié avec QuickPrep ou Sysprep, vous ne pouvez passer à l'autre méthode de personnalisation lorsque vous créez ou recomposez des postes de travail dans le pool.

Personnalisation de postes de travail de clone lié avec QuickPrep

Vous pouvez personnaliser les postes de travail de clone lié qui sont créés depuis une machine virtuelle parente en utilisant l'outil système QuickPrep. View Composer exécute QuickPrep lorsqu'un poste de travail de clone lié est créé ou recomposé.

QuickPrep personnalise un poste de travail de clone lié de plusieurs façons :

- Il donne à l'ordinateur un nom que vous spécifiez lorsque vous créez le pool de clone lié.
- Il crée un compte d'ordinateur dans Active Directory, en associant l'ordinateur au domaine approprié.
- Il monte le disque persistant de View Composer. Le profil d'utilisateur Windows est redirigé vers ce disque.
- Il redirige des fichiers temporaires et d'échange vers un disque séparé.

Ces étapes peuvent requérir un ou plusieurs redémarrages des clones liés.

QuickPrep utilise des clés de licence en volume KMS pour activer des postes de travail de clone lié Windows 8, Windows 7 et Windows Vista. Pour plus d'informations, reportez-vous à la section « Activation de Windows sur des postes de travail de clone lié », page 91.

Vous pouvez créer vos propres scripts pour personnaliser davantage les clones liés. QuickPrep peut exécuter deux types de scripts à des heures prédéfinies :

- après la création ou la recomposition des clones liés ;
- immédiatement avant la désactivation des clones liés.

Pour des recommandations et des règles sur l'utilisation de scripts de personnalisation QuickPrep, reportez-vous à la section « Exécution de scripts de personnalisation QuickPrep », page 119.

Remarque View Composer nécessite les informations d'identification d'un utilisateur de domaine pour associer des postes de travail de clone lié à un domaine Active Directory. Pour plus d'informations, reportez-vous à la section « Créer un compte d'utilisateur pour View Composer », page 15.

Exécution de scripts de personnalisation QuickPrep

Avec l'outil QuickPrep, vous pouvez créer des scripts pour personnaliser les postes de travail de clone lié dans un pool. Vous pouvez configurer QuickPrep pour exécuter des scripts de personnalisation à deux moments prédéfinis.

Lors de l'exécution de scripts QuickPrep

Le script de post-synchronisation s'exécute après la création, la recomposition ou le rééquilibrage des clones liés, et l'état du clone est **[Ready (Prêt)]** . Le script de désactivation s'exécute avant la désactivation de clones liés. Les scripts s'exécutent dans les systèmes d'exploitation client des clones liés.

Comment QuickPrep exécute des scripts

Le processus de QuickPrep utilise l'appel API `CreateProcess` de Windows pour exécuter des scripts. Votre script peut appeler n'importe quel processus pouvant être créé avec l'API `CreateProcess`. Par exemple, les processus `cmd`, `vbscript`, `exe` et de fichier de commandes fonctionnent avec l'API.

En particulier, QuickPrep transmet le chemin spécifié pour le script en tant que deuxième paramètre à l'API `CreateProcess` et définit le premier paramètre sur `NULL`.

Par exemple, si le chemin du script est `c:\myscript.cmd`, le chemin apparaît en tant que deuxième paramètre dans la fonction dans le fichier journal de View Composer : `CreateProcess(NULL,c:\myscript.cmd,...)`.

Fournir des chemins à des scripts QuickPrep

Vous fournissez des chemins aux scripts de personnalisation de QuickPrep lorsque vous créez un pool de postes de travail de clone lié ou lorsque vous modifiez des paramètres de personnalisation client d'un pool. Les scripts doivent résider sur la machine virtuelle parente. Vous ne pouvez pas utiliser de chemin d'accès UNC vers un partage de réseau.

Si vous utilisez un langage de script qui a besoin d'un interprète pour exécuter le script, le chemin du script doit démarrer par le binaire de l'interprète.

Par exemple, si vous spécifiez le chemin d'accès `C:\script\myvb.vbs` en tant que script de personnalisation QuickPrep, View Composer Agent ne peut pas exécuter le script. Vous devez spécifier un chemin qui démarre par le chemin du binaire de l'interprète :

```
C:\windows\system32\cscript.exe c:\script\myvb.vbs
```

Important Empêchez les utilisateurs ordinaires d'accéder aux scripts de personnalisation QuickPrep. Placez les scripts dans un dossier sécurisé.

Délai d'expiration du script QuickPrep

View Composer termine un script de post-synchronisation ou de désactivation qui prend plus de 20 secondes. Si votre script dure plus de 20 secondes, vous pouvez augmenter la limite d'expiration. Pour plus d'informations, reportez-vous à la section « Augmenter la limite du délai d'expiration des scripts de personnalisation QuickPrep », page 95.

Vous pouvez également utiliser votre script pour lancer un autre script ou processus exécutant la longue tâche.

Compte de script QuickPrep

QuickPrep exécute les scripts sous le compte dans lequel le service VMware View Composer Guest Agent Server est configuré pour être exécuté. Par défaut, ce compte est `système local`.

Ne modifiez pas ce compte d'ouverture de session. Si vous le faites, les clones liés ne démarrent pas.

Privilèges de processus QuickPrep

Pour des raisons de sécurité, certains privilèges du système d'exploitation Windows sont supprimés du processus View Composer Guest Agent qui appelle les scripts de personnalisation QuickPrep.

Un script de personnalisation QuickPrep ne peut pas exécuter des actions qui nécessitent un privilège qui est supprimé du processus View Composer Guest Agent.

Les privilèges suivants sont supprimés du processus qui appellent les scripts QuickPrep :

```
SeCreateTokenPrivilege
SeTakeOwnershipPrivilege
SeSecurityPrivilege
SeSystemEnvironmentPrivilege
SeLoadDriverPrivilege
SeSystemtimePrivilege
SeUndockPrivilege
SeManageVolumePrivilege
SeLockMemoryPrivilege
SeIncreaseBasePriorityPrivilege
SeCreatePermanentPrivilege
SeDebugPrivilege
SeAuditPrivilege
```

Journaux de script QuickPrep

Les journaux de View Composer contiennent des informations sur l'exécution du script QuickPrep. Le journal enregistre le début et la fin de l'exécution et journalise des messages de sortie ou d'erreur. Le journal se trouve dans le répertoire `temp` de Windows :

```
C:\Windows\Temp\vmware-viewcomposer-ga-new.log
```

Recomposition de clones liés personnalisés avec Sysprep

Si vous recomposez un poste de travail de clone lié personnalisé avec Sysprep, View Manager exécute de nouveau la spécification de personnalisation Sysprep après la recomposition du disque du système d'exploitation. Cette opération génère un nouveau SID pour la machine virtuelle de clone lié.

Si un nouveau SID est généré, le clone lié recomposé fonctionne comme un nouvel ordinateur sur le réseau. Certains programmes logiciels, tels que des outils de gestion système, dépendent du SID pour identifier les ordinateurs qu'ils gèrent. Ces programmes peuvent ne pas pouvoir identifier ou rechercher la machine virtuelle de clone lié.

De plus, si un logiciel tiers est installé sur le disque système, la spécification de personnalisation peut regénérer les GUID de ce logiciel après la recomposition.

Une recomposition restaure le clone lié à son état d'origine, avant la première exécution de la spécification de personnalisation. Dans cet état, le clone lié ne possède pas de SID d'ordinateur local ou le GUID des logiciels tiers installés sur le lecteur système. View Manager doit exécuter la spécification de personnalisation Sysprep après la recomposition du clone lié.

Dimensionnement du stockage pour des pools de postes de travail de clone lié

View Manager offre des recommandations très utiles qui peuvent vous aider à déterminer quelle quantité de stockage est requise pour un pool de postes de travail de clone lié. Un tableau dans l'assistant Ajouter un pool montre une estimation générale des exigences de stockage des disques de clone lié lors de la création du pool et tout au long de la croissance des clones liés.

Le tableau de dimensionnement du stockage affiche également l'espace libre sur les magasins de données que vous sélectionnez pour le stockage de disques du système d'exploitation, de disques persistants de View Composer et de réplicas. Vous pouvez décider des magasins de données à utiliser en comparant l'espace libre réel et les exigences estimées pour les disques de clone lié.

Les formules que View Manager utilise ne peuvent fournir qu'une estimation générale de l'utilisation de stockage. La croissance de stockage réelle de vos clones liés dépend de nombreux facteurs :

- Quantité de mémoire affectée à la machine virtuelle parente
- Fréquence des opérations d'actualisation
- Taille du fichier d'échange du système d'exploitation client
- Si vous redirigez des fichiers temporaires et d'échange vers un disque séparé
- Si vous configurez des disques persistants de View Composer séparés
- Charge de travail sur les postes de travail de clone lié, déterminée principalement par les types d'applications que les utilisateurs exécutent sur le système d'exploitation client

---

Remarque Dans un déploiement qui inclut des centaines ou des milliers de clones liés, configurez vos pools de clone lié pour que des ensembles particuliers de magasins de données soient dédiés à des clusters ESX particuliers. Ne configurez pas de pools de manière aléatoire sur tous les magasins de données pour que la plupart ou tous les hôtes ESX doivent accéder à la plupart ou à tous les LUN.

Lorsque trop d'hôtes ESX tentent d'écrire à des disques du système d'exploitation de clone lié sur un LUN particulier, des problèmes de contention peuvent se produire, ce qui dégrade les performances et interfère avec l'évolutivité. Pour plus d'informations sur la planification du magasin de données dans des déploiements volumineux, consultez le document *Planification de l'architecture de VMware Horizon View*.

Recommandations sur le dimensionnement des pools de clone lié

Lorsque vous créez ou modifiez un pool de postes de travail de clone lié, la page **[Select Datastores (Sélectionner des magasins de données)]** affiche un tableau avec des recommandations sur le dimensionnement du stockage. Le tableau peut vous aider à décider des magasins de données à sélectionner pour les disques de clone lié.

Tableau de dimensionnement des disques de clone lié

Tableau 5-7 montre un exemple de recommandations de dimensionnement du stockage pouvant s'afficher pour un pool de 10 machines virtuelles si la machine virtuelle parente dispose de 1 Go de mémoire et d'un réplica de 10 Go. Dans cet exemple, différents magasins de données sont sélectionnés pour les disques du système d'exploitation et les disques persistants de View Composer.

Tableau 5-7. Exemple de tableau de dimensionnement des disques de clone lié

Type de données	Espace libre sélectionné (Go)	Min. recommandé (Go)	Utilisation 50 % (Go)	Max. recommandé (Go)
disques du système d'exploitation	184,23	40	80	130
Persistent disks (Disques persistants)	28,56	4	10	20

La colonne **[Selected Free Space (Espace libre sélectionné)]** montre l'espace disponible total sur tous les magasins de données que vous avez sélectionnés pour un type de disque, tel que des disques du système d'exploitation.

La colonne **[Min Recommended (Min. recommandé)]** indique la quantité minimale de stockage recommandé pour un pool.

La colonne **[50% Utilization (Utilisation 50 %)]** montre le stockage recommandé lorsque des disques de clone lié atteignent 50 % de la machine virtuelle parente.

La colonne **[Max Recommended (Max. recommandé)]** montre le stockage recommandé lorsque des disques de clone lié approchent de la taille complète de la machine virtuelle parente.

Si vous stockez des disques du système d'exploitation et des disques persistants sur le même magasin de données, View Manager calcule les exigences de stockage des deux types de disque. Le **[Data Type (Type de données)]** indique **[Linked clones (Clones liés)]** plutôt qu'un type de disque particulier.

Si vous stockez des réplicas View Composer sur un magasin de données séparé, le tableau montre également des recommandations de stockage pour les réplicas et ajuste les recommandations pour les disques du système d'exploitation.

Recommandations sur le dimensionnement

Le tableau fournit des recommandations générales. Vos calculs de stockage doivent prendre en compte des facteurs supplémentaires qui peuvent affecter la croissance du stockage réel dans le pool de clone lié.

Pour les disques du système d'exploitation, vos estimations de dimensionnement dépendent de la fréquence à laquelle vous actualisez et recomposez le pool.

Si vous actualisez votre pool de clone lié entre une fois par jour et une fois par semaine, assurez-vous que le **[Selected Free Space (Espace libre sélectionné)]** peut s'adapter à l'utilisation du stockage entre les estimations de **[Min Recommended (Min. recommandé)]** et **[50% Utilization (Utilisation 50 %)]** .

Si vous actualisez ou recomposez rarement le pool, les disques de clone lié continuent de croître. Assurez-vous que le **[Selected Free Space (Espace libre sélectionné)]** peut s'adapter à l'utilisation de stockage entre les estimations de **[50 % Utilization (Utilisation 50 %)]** et **[Max Recommended (Max. recommandé)]** .

Pour les disques persistants, vos estimations de dimensionnement dépendent de la quantité de données de profil Windows générées par les utilisateurs sur leurs postes de travail. Les opérations d'actualisation et de recomposition n'affectent pas les disques persistants.

Comment View Manager calcule les recommandations de dimensionnement minimales

Pour arriver à une recommandation minimale pour les disques du système d'exploitation, View Manager estime que chaque clone consomme deux fois sa taille de mémoire lors de sa création et de son premier démarrage. Si aucune mémoire n'est réservée pour un clone, un fichier d'échange ESX est créé pour un clone dès qu'il est activé. La taille du fichier d'échange du système d'exploitation client affecte également la croissance d'un disque du système d'exploitation d'un clone.

Dans les recommandations minimales pour les disques du système d'exploitation, View Manager inclut également de l'espace pour deux réplicas sur chaque magasin de données. View Composer crée un réplica lorsqu'un pool est créé. Lorsque le pool est recomposé pour la première fois, View Composer crée un deuxième réplica sur le magasin de données, ancre les clones liés au nouveau réplica et supprime le premier réplica si aucun autre clone n'utilise le snapshot d'origine. Le magasin de données doit avoir la capacité de stocker deux réplicas au cours de l'opération de recomposition.

Par défaut, les réplicas utilisent l'approvisionnement fin de vSphere, mais pour garder les recommandations simples, View Manager prend en compte deux réplicas qui utilisent le même espace que la machine virtuelle parente.

Pour arriver à une recommandation minimale pour des disques persistants, View Manager calcule 20 % de la taille de disque que vous spécifiez sur la page **[View Composer Disks (Disques de View Composer)]** de l'assistant Add Pool (Ajouter un pool).

Remarque Les calculs pour les disques persistants sont basés sur des valeurs de seuil statique, en gigaoctets. Par exemple, si vous spécifiez la taille du disque persistant d'une valeur comprise entre 1 024 Mo et 2 047 Mo, View Manager calcule la taille de disque persistant sur 1 Go. Si vous spécifiez une taille de disque de 2 048 Mo, View Manager calcule la taille de disque sur 2 Go.

Pour arriver à une recommandation pour le stockage de réplicas sur un magasin de données séparé, View Manager alloue de l'espace pour deux réplicas sur le magasin de données. La même valeur est calculée pour l'utilisation minimale et maximale.

Pour plus d'informations, reportez-vous à la section « Formules de dimensionnement des pools de clone lié », page 123.

Recommandations sur le dimensionnement et surcharge de stockage

Une fois que vous avez estimé des exigences de stockage, sélectionné des magasins de données et déployé le pool, View Manager approvisionne des machines virtuelles de clone lié sur des magasins de données différents en fonction de l'espace libre et des clones existants sur chaque magasin de données.

En fonction de l'option de surcharge de stockage que vous sélectionnez sur la page **[Select Datastores (Sélectionner des magasins de données)]** dans l'assistant Add Pool (Ajouter un pool), View Manager arrête d'approvisionner de nouveaux clones et réserve de l'espace libre pour les clones existants. Ce comportement garantit l'existence d'une mémoire tampon de croissance pour chaque poste de travail sur le magasin de données.

Si vous sélectionnez un niveau de surcharge de stockage agressif, les exigences de stockage estimées peuvent dépasser la capacité indiquée dans la colonne **[Selected Free Space (Espace libre sélectionné)]** . Le niveau de surcharge de stockage affecte le nombre de machines virtuelles que View Manager crée réellement sur un magasin de données.

Pour plus d'informations, reportez-vous à la section « Définir le niveau de surcharge de stockage pour des postes de travail de clone lié », page 125.

Formules de dimensionnement des pools de clone lié

Des formules de dimensionnement du stockage peuvent vous aider à estimer la taille de disques de clone lié relative à l'espace libre sur les magasins de données que vous sélectionnez pour les disques du système d'exploitation, les disques persistants de View Composer et les réplicas.

Formules de dimensionnement du stockage

Tableau 5-8 montre les formules qui calculent les tailles estimées de disques de clone lié lors de la création d'un pool et tout au long de la croissance des postes de travail de clone lié. Ces formules incluent l'espace des disques de réplica stockés avec les clones sur le magasin de données.

Si vous modifiez un pool existant ou que vous stockez des réplicas sur un magasin de données séparé, View Manager utilise une formule de dimensionnement différente. Pour plus d'informations sur la configuration de connexions directes, reportez-vous à la section « Formules de dimensionnement pour créer des clones liés lorsque vous modifiez un pool ou stockez des réplicas sur un magasin de données séparé », page 124.

Tableau 5-8. Formules de dimensionnement du stockage des disques de clone lié sur des magasins de données sélectionnés

Type de données	Espace libre sélectionné (Go)	Min. recommandé (Go)	Utilisation 50 % (Go)	Max. recommandé (Go)
disques du système d'exploitation	Espace libre sur les magasins de données sélectionnés	Nombre de VM * (2 * mémoire de VM) + (2 * disque de réplica)	Nombre de VM * (50 % de disque de réplica + mémoire de VM) + (2 * disque de réplica)	Nombre de VM * (100 % de disque de réplica + mémoire de VM) + (2 * disque de réplica)
Persistent disks (Disques persistants)	Espace libre sur les magasins de données sélectionnés	Nombre de VM * 20 % de disque persistant	Nombre de VM * 50 % de disque persistant	Nombre de VM * 100 % de disque persistant

Exemple d'estimation de dimensionnement du stockage

Dans cet exemple, la machine virtuelle parente est configurée avec 1 Go de mémoire. La taille de disque de la machine virtuelle parente est de 10 Go. Un pool de clone lié est créé avec 10 postes de travail. Des disques persistants sont configurés avec une taille de 2 048 Mo.

Les disques du système d'exploitation sont configurés sur un magasin de données dont l'espace disponible est actuellement de 184,23 Go. Les disques persistants sont configurés sur un magasin de données différent avec 28,56 Go d'espace disponible.

Tableau 5-9 montre comment les formules de dimensionnement calculent des exigences de stockage estimées pour le pool de clone lié en exemple.

Tableau 5-9. Exemple d'estimation de dimensionnement des disques de clone lié déployés sur des magasins de données sélectionnés

Type de données	Espace libre sélectionné (Go)	Min. recommandé (Go)	Utilisation 50 % (Go)	Max. recommandé (Go)
disques du système d'exploitation	184,23	10 * (2*1 Go) + (2*10 Go) = 40	10 * (50 % de 10 Go + 1 Go) + (2*10 Go) = 80	10 * (100 % de 10 Go + 1 Go) + (2*10 Go) = 130
Persistent disks (Disques persistants)	28,56	10 * (20 % de 2 Go) = 4	10 * (50 % de 2 Go) = 10	10 * (100 % de 2 Go) = 20

Formules de dimensionnement pour créer des clones liés lorsque vous modifiez un pool ou stockez des réplicas sur un magasin de données séparé

View Manager calcule différentes formules de dimensionnement lorsque vous modifiez un pool de clone lié existant, ou lorsque vous stockez des réplicas sur un magasin de données séparé, plutôt que lorsque vous créez un pool.

Si vous modifiez un pool existant et que vous sélectionnez des magasins de données pour le pool, View Composer crée de nouveaux clones sur les magasins de données sélectionnés. Les nouveaux clones sont ancrés au snapshot existant et utilisent le disque de réplica existant. Aucun nouveau réplica n'est créé.

Si vous stockez des réplicas sur un magasin de données séparé, les autres magasins de données sélectionnés sont dédiés aux disques de clone lié.

Dans ces cas-là, View Manager n'inclut pas d'espace pour des réplicas lorsqu'il calcule des recommandations de stockage pour des disques de clone lié.

Tableau 5-10 montre les formules qui calculent les tailles estimées de disques de clone lié lorsque vous modifiez un pool ou stockez des réplicas sur un magasin de données séparé.

Tableau 5-10. Formules de dimensionnement du stockage des disques de clone lié lorsque vous modifiez un pool ou stockez des réplicas sur un magasin de données séparé

Type de données	Espace libre sélectionné (Go)	Min. recommandé (Go)	Utilisation 50 % (Go)	Max. recommandé (Go)
disques du système d'exploitation	Espace libre sur les magasins de données sélectionnés	Nombre de VM * (2 * mémoire de VM)	Nombre de VM * (50 % de disque de réplica + mémoire de VM)	Nombre de VM * (100 % de disque de réplica + mémoire de VM)
Persistent disks (Disques persistants)	Espace libre sur les magasins de données sélectionnés	Nombre de VM * 20 % de disque persistant	Nombre de VM * 50 % de disque persistant	Nombre de VM * 100 % de disque persistant

Exemple d'estimation de dimensionnement du stockage lorsque vous modifiez un pool ou stockez des réplicas sur un magasin de données séparé

Dans cet exemple, la machine virtuelle parente est configurée avec 1 Go de mémoire. La taille de disque de la machine virtuelle parente est de 10 Go. Un pool de clone lié est créé avec 10 postes de travail. Des disques persistants sont configurés avec une taille de 2 048 Mo.

Les disques du système d'exploitation sont configurés sur un magasin de données dont l'espace disponible est actuellement de 184,23 Go. Les disques persistants sont configurés sur un magasin de données différent avec 28,56 Go d'espace disponible.

Tableau 5-11 montre comment les formules de dimensionnement calculent des exigences de stockage estimées pour le pool de clone lié en exemple.

Tableau 5-11. Exemple d'estimation de dimensionnement des disques de clone lié lorsque vous modifiez un pool ou stockez des réplicas sur un magasin de données séparé

Type de données	Espace libre sélectionné (Go)	Min. recommandé (Go)	Utilisation 50 % (Go)	Max. recommandé (Go)
disques du système d'exploitation	184,23	10 * (2*1 Go) = 20	10 * (50 % de 10 Go + 1 Go) = 60	10 * (100 % de 10 Go + 1 Go) = 110
Persistent disks (Disques persistants)	28,56	10 * (20 % de 2 Go) = 4	10 * (50 % de 2 Go) = 10	10 * (100 % de 2 Go) = 20

Définir le niveau de surcharge de stockage pour des postes de travail de clone lié

Vous pouvez contrôler le niveau d'agressivité auquel View Manager crée des postes de travail de clone lié sur un magasin de données en utilisant la fonction de surcharge de stockage. Cette fonction vous permet de créer des clones liés ayant une taille logique totale supérieure à la limite de stockage physique du magasin de données.

Cette fonction ne fonctionne qu'avec des pools de clone lié.

Le niveau de surcharge de stockage calcule la quantité de stockage supérieure à la taille physique du magasin de données que les clones utiliseraient si chaque clone était une machine virtuelle complète. Pour plus d'informations, reportez-vous à la section « Surcharge de stockage des postes de travail de clone lié », page 126.

Procédure

1 Dans View Administrator, cliquez sur **[Inventory (Inventaire)] > [Pools]** .

2 Lorsque vous créez un nouveau pool de postes de travail ou que vous modifiez un pool existant, allez à la page Select Datastores (Sélectionner des magasins de données).

Option	Action
New desktop pool (Nouveau pool de postes de travail)	a Cliquez sur **[Add (Ajouter)]** . b Continuez l'assistant Add Pool (Ajouter un pool) jusqu'à la page Select Datastores (Sélectionner des magasins de données).
Existing desktop pool (Pool de postes de travail existant)	a Sélectionnez le pool de clone lié et cliquez sur **[Edit (Modifier)]** . b Cliquez sur l'onglet **[vCenter Settings (Paramètres de vCenter)]** .

3 Sur la page Select Datastores (Sélectionner des magasins de données), sélectionnez le niveau de surcharge de stockage.

Option	Description
None (Aucun)	Le stockage n'est pas surchargé.
Conservative (Conservateur)	4 fois la taille du magasin de données. Il s'agit du niveau par défaut.
Moderate (Modéré)	7 fois la taille du magasin de données.
Aggressive (Agressif)	15 fois la taille du magasin de données.

4 Cliquez sur **[Done (Terminé)]** .

5 Cliquez sur **[Finish (Terminer)]** .

Surcharge de stockage des postes de travail de clone lié

Avec la fonction de surcharge de stockage, vous pouvez réduire les coûts de stockage en plaçant plus de postes de travail de clone lié sur un magasin de données qu'il n'est possible avec des postes de travail de machine virtuelle complets. Les clones liés peuvent utiliser un espace de stockage logique plusieurs fois supérieur à la capacité physique du magasin de données.

Cette fonction vous aide à choisir un niveau de stockage qui vous permet de surcharger la capacité du magasin de données et définit une limite pour le nombre de clones liés que View Manager crée. Vous pouvez éviter de gaspiller du stockage en approvisionnant de façon trop conservatrice ou éviter de risquer que les clones liés n'aient plus d'espace disque et provoquent l'échec de leurs applications de poste de travail.

Par exemple, vous pouvez créer au plus dix machines virtuelles complètes sur un magasin de données de 100 Go, si chaque machine virtuelle est de 10 Go. Lorsque vous créez des clones liés à partir d'une machine virtuelle parente de 10 Go, chaque clone est une fraction de cette taille.

Si vous définissez un niveau de surcharge conservateur, View Manager permet aux clones d'utiliser quatre fois la taille physique du magasin de données, en mesurant chaque clone comme s'il était de la taille de la machine virtuelle parente. Sur un magasin de données de 100 Go, avec un parent de 10 Go, View Manager approvisionne environ 40 clones liés. View Manager n'approvisionne pas plus de clones, même si le magasin de données a de l'espace libre. Cette limite conserve une mémoire tampon de croissance pour les clones existants.

Tableau 5-12 montre les niveaux de surcharge de stockage que vous pouvez définir.

Tableau 5-12. Niveaux de surcharge de stockage

Option	Niveau de surcharge de stockage
None (Aucun)	Le stockage n'est pas surchargé.
Conservative (Conservateur)	4 fois la taille du magasin de données. Il s'agit du niveau par défaut.
Moderate (Modéré)	7 fois la taille du magasin de données.
Aggressive (Agressif)	15 fois la taille du magasin de données.

Les niveaux de surcharge de stockage permettent de déterminer la capacité de stockage de façon très efficace. Pour déterminer le meilleur niveau, surveillez la croissance des clones liés dans votre environnement.

Définissez un niveau agressif si vos disques du système d'exploitation n'atteignent jamais leur taille maximale possible. Un niveau de surcharge agressif demande de l'attention. Pour vous assurer que les clones liés ne manquent pas d'espace disque, vous pouvez périodiquement actualiser ou rééquilibrer le pool de postes de travail et réduire les données de système d'exploitation des clones liés à leur taille d'origine.

Par exemple, il est logique de définir un niveau de surcharge agressif pour un pool de postes de travail d'affectation flottante dans lequel les postes de travail sont définis pour être supprimés ou actualisés après la fermeture de session.

Vous pouvez varier les niveaux de surcharge de stockage parmi les différents types de magasins de données pour cibler différents niveaux de débit dans chaque magasin de données. Par exemple, un magasin de données NAS peut avoir un paramètre différent d'un magasin de données SAN.

Stockage des postes de travail de clone liés dans des magasins de données locaux

Les postes de travail de clone lié peuvent être stockés dans des magasins de données locaux qui sont des disques de rechange internes dans les hôtes ESXi. Le stockage local offre des avantages, tels que la possibilité d'utiliser un matériel économique, le provisionnement rapide des machines virtuelles, des opérations d'alimentation hautes performances et une gestion simplifiée. Cependant, le stockage local limite les options de configuration de l'infrastructure vSphere dont vous pouvez disposer. Le stockage local offre des avantages dans certains environnements View, mais pas dans d'autres.

L'utilisation de magasins de données locaux est probablement plus efficace si les postes de travail View sont des postes de travail sans état dans l'environnement. Par exemple, vous pouvez utiliser des magasins de données locaux si vous déployez des kiosques sans état ou des postes de salle de classe ou de formation.

Utilisez des magasins de données locaux si les postes de travail ont des affectations flottantes, ne sont pas dédiés à des utilisateurs finaux, ne nécessitent pas des disques persistants pour les données utilisateur et peuvent être supprimés ou actualisés régulièrement lors de la fermeture de session de l'utilisateur, par exemple. Cette approche permet de contrôler l'utilisation des disques de chaque magasin de données local sans avoir à transférer ou équilibrer la charge des machines virtuelles dans les magasins de données.

Cependant, vous devez tenir compte des restrictions que les magasins de données locaux imposent sur le déploiement de poste de travail View :

- Vous ne pouvez pas utiliser VMotion pour gérer les volumes.
- Vous ne pouvez pas équilibrer la charge des machines virtuelles dans un pool de ressources. Par exemple, vous ne pouvez pas utiliser l'équilibrage de charge View Composer avec des clones liés stockés dans des magasins de données locaux.
- Vous ne pouvez pas utiliser VMware High Availability.
- Vous ne pouvez pas utiliser DRS (vSphere Distributed Resource Scheduler).
- Vous ne pouvez pas stocker un réplica View Composer et les clones cliés dans des magasins de données distincts si le réplica se trouve dans un magasin de données local.

  Lorsque vous stockez les clones liés dans des magasins de données locaux, VMware recommande vivement de stocker le réplica dans le même volume que les clones liés. Bien qu'il soit possible de stocker les clones liés dans des magasins de données locaux et le réplica dans un magasin de données partagé si tous les hôtes ESXi du cluster peuvent accéder à le réplica, VMware déconseille cette configuration.
- Si vous sélectionnez des unités de disque rotatives, les performances peuvent ne pas être identiques à celles d'une baie de stockage disponible dans le commerce. Les unités de disque rotatives locales et une baie de stockage peuvent avoir des capacités similaires, mais les premières n'offrent pas le même débit que la baie de stockage. Le débit augmente proportionnellement avec le nombre de piles.

Si vous sélectionnez des disques électroniques (SSD) connectés directement, les performances seront vraisemblablement meilleures que celles de la plupart des baies de stockage.

Vous pouvez stocker les clones liés dans des magasins de données locaux sans contraintes si vous configurez le pool de postes de travail sur un seul hôte ESXi ou dans un cluster qui contient un seul hôte ESXi. Cependant, l'utilisation d'un seul hôte ESXi limite la taille du pool de postes de travail que vous pouvez configurer.

Pour configurer un grand pool de postes de travail, vous devez sélectionner un cluster qui contient plusieurs hôtes ESXi ayant une capacité collective permettant de prendre en charge un grand nombre de machines virtuelles.

Si vous voulez tirer parti des avantages du stockage local, vous devez soigneusement tenir compte des conséquences de l'impossibilité d'utiliser VMotion, HA, DRS et d'autres fonctions. Si vous gérez l'utilisation des disques locaux en contrôlant le nombre de disques des machines virtuelles et la croissance des disques, vous pouvez déployer avec succès les clones liés dans des magasins de données locaux si vous utilisez des affectations flottantes et exécutez régulièrement des opérations d'actualisation et de suppression.

Stockage de réplicas et de clones liés View Composer sur des magasins de données séparés

Vous pouvez placer des réplicas et des clones liés View Composer sur des magasins de données séparés avec différentes caractéristiques de performance. Cette configuration flexible peut accélérer les opérations intensives telles que l'approvisionnement de plusieurs clones liés à la fois ou l'exécution d'une analyse antivirus.

Par exemple, vous pouvez stocker les machines virtuelles réplicas sur un magasin de données sur disque électronique. Les disques électroniques ont une capacité de stockage faible et des performances de lecture élevées. Ils prennent en charge généralement 20 000 E/S par seconde (IOPS). View Composer ne crée qu'une seul réplica pour chaque snapshot d'image de base View Composer sur chaque cluster ESX et les réplicas ne requièrent donc pas autant d'espace de stockage. Un disque électronique peut augmenter la vitesse à laquelle ESXi lit le disque du système d'exploitation d'une réplica quand une tâche est effectuée simultanément sur plusieurs clones liés.

Vous pouvez stocker des clones liés sur des magasins de données sur des supports de rotation traditionnels. Ces disques fournissent des performances inférieures et prennent en charge en général 200 IOPS. Ils sont bon marché et fournissent une capacité de stockage élevée. Ils sont donc adaptés pour le stockage des nombreux clones liés d'un pool volumineux. ESXi n'a pas à effectuer des opérations de lecture simultanées intensives sur un clone lié.

La configuration de réplicas et de clones liés de cette façon peut réduire l'impact des tempêtes d'E/S qui se produisent quand de nombreux clones liés sont créés à la fois. Par exemple, si vous déployez un pool d'affectation flottante avec une règle de « suppression du poste de travail à la fermeture de session », et que vos utilisateurs commencent à travailler en même temps, View Manager doit approvisionner simultanément de nouveaux postes de travail pour eux.

Important Cette fonction est conçue pour des configurations de stockage spécifiques de fournisseurs qui offrent des solutions de disque haute performance. Ne stockez pas de réplicas sur un magasin de données séparé si votre matériel de stockage ne prend pas en charge les performances de lecture élevées.

Vous devez satisfaire certaines exigences lorsque vous stockez le réplica et les clones liés d'un pool sur des magasins de données séparés :

- Vous ne pouvez spécifier qu'un magasin de données réplica séparé pour chaque pool.
- Si un magasin de données de réplica est partagé, il doit être accessible depuis tous les hôtes ESXi du cluster.
- Si les magasins de données de clone lié sont partagés, le magasin de données réplica doit être partagé. le réplica ne peut pas se trouver dans un magasin de données local.

Si les magasins de données de clone lié sont locaux, VMware recommande vivement de stocker le réplica sur le même volume que les clones liés. Bien qu'il soit possible de stocker les clones liés dans des magasins de données locaux et le réplica dans un magasin de données partagé si tous les hôtes ESXi du cluster peuvent accéder à le réplica, VMware déconseille cette configuration.

Considérations sur la disponibilité pour le stockage de réplicas sur un magasin de données séparé ou des magasins de données partagés

Vous pouvez stocker des réplicas View Composer sur un magasin de données séparé ou sur les mêmes magasins de données que des machines virtuelles de clone lié. Ces configurations affectent la disponibilité du pool de différentes façons.

Lorsque vous stockez des réplicas sur les mêmes magasins de données que les clones liés, View Composer crée un réplica séparé sur chaque magasin de données pour améliorer la disponibilité. Si un magasin de données devient indisponible, seuls les clones liés sur ce magasin de données sont affectés. Les clones liés sur d'autres magasins de données sont toujours exécutés.

Lorsque vous stockez des réplicas sur un magasin de données séparé, tous les clones liés du pool sont ancrés aux réplicas sur ce magasin de données. Si le magasin de données devient indisponible, l'intégralité du pool est indisponible.

Pour améliorer la disponibilité des postes de travail de clone lié, vous pouvez configurer une solution hautement disponible pour le magasin de données sur lequel vous stockez les réplicas.

Utilisation de View Composer Array Integration avec la technologie de snapshot NFS natif (VAAI)

Si votre déploiement inclut des périphériques NAS qui prennent en charge VAAI (vStorage APIs for Array Integration), vous pouvez activer la fonction View Composer Array Integration sur des pools de clone lié. Cette fonction utilise la technologie de snapshot NFS natif pour cloner des machines virtuelles.

Remarque La technologie de snapshot NFS natif (VAAI) est une fonction de la présentation technique. La fonction est disponible à l'essai, mais il n'est pas conseillé de l'utiliser en production et aucun support n'est fourni.

Avec cette technologie, la baie de disques NFS clone les fichiers de la machine virtuelle sans demander à l'hôte ESXi de lire et d'écrire les données. Cette opération peut réduire la durée et la charge réseau nécessaires lors du clonage de machines virtuelles.

Appliquez ces recommandations à l'utilisation de la technologie de snapshot NFS natif :

- Vous pouvez utiliser cette fonction uniquement si vous configurez des pools de postes de travail sur des magasins de données résidant sur des périphériques NAS prenant en charge les opérations de clonage natif via VAAI.
- Vous pouvez utiliser des fonctions de View Composer pour gérer des clones liés qui sont créés par la technologie de snapshot NFS natif. Par exemple, vous pouvez actualiser, recomposer, rééquilibrer, créer des disques persistants et exécuter des scripts de personnalisation QuickPrep sur ces clones.
- Vous ne pouvez pas utiliser cette fonction si vous stockez des réplicas et des disques du système d'exploitation sur des magasins de données séparés.
- Cette fonction est prise en charge sur vSphere 5.0 et supérieur.
- Vous pouvez utiliser des machines virtuelles clonées par un périphérique NAS en mode local. Toutefois, lorsque des utilisateurs empruntent leurs postes de travail, l'image de base de View Composer dans le référentiel de Serveur de transfert n'est pas utilisée dans l'opération d'emprunt. Au lieu de cela, Serveur de transfert View monte et télécharge l'ensemble de la machine virtuelle sur l'ordinateur client.

Une fois qu'un utilisateur restitue un poste de travail, le clonage NFS natif n'est pas réutilisé pour ce poste de travail. View gère le poste de travail comme une machine virtuelle complète. Cette contrainte s'applique uniquement aux postes de travail qui ont été utilisés en mode local. Les postes de travail distants dans le pool continuent de bénéficier du clonage NFS natif.

- Si vous modifiez un pool et si vous sélectionnez ou désélectionnez la fonction de clonage NFS native, des machines virtuelles existantes ne sont pas affectées.

  Pour modifier des machines virtuelles existantes de clones NFS natifs en clones de fichiers journaux traditionnels, vous devez désélectionner la fonction de clonage NFS natif et recomposer le pool vers une nouvelle image de base. Pour modifier la méthode de clonage pour toutes les machines virtuelles dans un pool et utiliser un magasin de données différent, vous devez sélectionner le nouveau magasin de données, désélectionner la fonction de clonage NFS natif, rééquilibrer le pool vers le nouveau magasin de données et recomposer le pool vers une nouvelle image de base.

  De la même façon, pour modifier des machines virtuelles de clones de fichiers journaux traditionnels en clones NFS natifs, vous devez sélectionner un magasin de données NAS prenant en charge VAAI, sélectionner la fonction de clonage NFS natif, rééquilibrer le pool vers le magasin de données NAS et recomposer le pool.

- Sur un cluster ESXi, pour configurer le clonage natif sur un magasin de données NFS sélectionné dans View Administrator, vous devrez peut-être installer des plug-ins NAS spécifiques du fournisseur qui prennent en charge les opérations de clonage natif sur VAAI sur tous les hôtes ESXi dans le cluster. Pour plus d'informations sur les exigences de configuration, consultez la documentation de votre fournisseur de stockage.

- La technologie de snapshot NFS natif (VAAI) n'est pas prise en charge dans les pools activés pour View Storage Accelerator ou pour la récupération d'espace disque de machine virtuelle.

IMPORTANT Les fournisseurs de stockage NAS peuvent fournir des paramètres supplémentaires qui peuvent affecter les performances et le fonctionnement de VAAI. Vous devez suivre les recommandations du fournisseur et configurer les paramètres appropriés sur la baie de stockage NAS et ESXi. Pour plus d'informations sur la configuration des paramètres recommandés par le fournisseur, consultez la documentation de votre fournisseur de stockage.

Récupérer de l'espace disque sur des postes de travail de clone lié

Dans vSphere 5.1 et supérieur, vous pouvez configurer la fonction de récupération d'espace disque pour les pools de postes de travail de clone lié. À partir de vSphere 5.1, View crée des machines virtuelles de clone lié dans un format de disque efficace qui permet à des hôtes ESXi de récupérer l'espace disque inutilisé sur les clones liés, ce qui réduit l'espace de stockage total requis pour les clones liés.

Comme les utilisateurs interagissent avec des postes de travail de clone lié, les disques du système d'exploitation des clones croissent et peuvent finir par utiliser presque autant d'espace disque que les postes de travail de clone complet. La récupération d'espace disque réduit la taille des disques du système d'exploitation sans que vous ayez à actualiser ou recomposer les clones liés. L'espace peut être récupéré lorsque les machines virtuelles sont activées et que les utilisateurs interagissent avec leurs postes de travail.

Dans View Administrator, vous ne pouvez pas initier directement la récupération d'espace disque pour un pool. Vous déterminez le moment auquel View initie la récupération d'espace disque en spécifiant la quantité minimale d'espace disque inutilisé qui doit être atteinte sur un disque du système d'exploitation de clone lié pour déclencher l'opération. Lorsque l'espace disque inutilisé dépasse le seuil spécifié, View demande à l'hôte ESXi de récupérer l'espace sur ce disque du système d'exploitation. View applique le seuil sur chaque machine virtuelle dans le pool.

Vous pouvez utiliser l'option `vdmadmin -M` pour initier la récupération d'espace disque sur une machine virtuelle particulière à des fins de démonstration ou de dépannage. Reportez-vous à la section « Récupération d'espace disque sur des machines virtuelles à l'aide de l'option -M », page 478.

Vous pouvez configurer la récupération d'espace disque sur des clones liés lorsque vous créez un nouveau pool ou lorsque vous modifiez un pool existant. Pour un pool existant, consultez la section « Mettre à niveau des pools de postes de travail pour la récupération d'espace » dans le document *Mises à niveau de VMware Horizon View*.

Si View Composer actualise, recompose ou rééquilibre des clones liés, la récupération d'espace disque n'a pas lieu sur ces clones liés.

La récupération d'espace disque fonctionne uniquement sur les disques du système d'exploitation dans des clones liés. La fonction n'affecte pas les disques persistants de View Composer et ne fonctionne pas sur les machines virtuelles de clone complet.

La technologie de snapshot NFS natif (VAAI) n'est pas prise en charge dans les pools contenant des machines virtuelles avec des disques à optimisation d'espace.

Prérequis

- Vérifiez que vos hôtes de vCenter Server et ESXi sont à la version 5.1 avec le correctif de téléchargement ESXi 5.1 ESXi510-201212001 ou supérieur.

  Dans un cluster ESXi, vérifiez que tous les hôtes sont à la version 5.1 avec le correctif de téléchargement ESXi510-201212001 ou supérieur.
- Vérifiez que VMware Tools fourni avec vSphere 5.1 ou supérieur est installé sur toutes les machines virtuelles de cloné lié dans le pool.
- Vérifiez que toutes les machines virtuelles de cloné lié dans le pool ont la version matérielle virtuelle 9 ou supérieure.
- Vérifiez que les machines virtuelles utilisent des contrôleurs SCSI. La récupération d'espace disque n'est pas prise en charge sur les machines virtuelles avec des contrôleurs IDE.
- Vérifiez que les postes de travail de clone lié exécutent Windows XP ou Windows 7. La récupération d'espace disque n'est pas prise en charge sur les postes de travail Windows 8.
- Vérifiez que la récupération d'espace disque est activée dans vCenter Server. Cette option garantit que les machines virtuelles dans le pool sont créées au format de disque efficace requis pour récupérer l'espace disque. Reportez-vous à la section « Autoriser vSphere à récupérer de l'espace disque dans des machines virtuelles de clone lié », page 20.

Procédure

1 Dans View Administrator, affichez la page Options de stockage avancées.

Option	Description
Nouveau pool de postes de travail	Démarrez l'assistant Ajouter un pool pour commencer la création d'un pool de postes de travail automatisé. Suivez les invites de configuration de l'assistant jusqu'à la page Options de stockage avancées.
Pool de postes de travail existant	Sélectionnez le pool existant, cliquez sur **[Modifier]** et cliquez sur l'onglet **[Options de stockage avancées]** . Pour mettre à niveau un pool afin qu'il prenne en charge la récupération d'espace, consultez la section « Mettre à niveau des pools de postes de travail pour la récupération d'espace » dans le document *Mises à niveau de VMware Horizon View*.

2 Cochez la case **[Récupérer l'espace disque de machine virtuelle]** .

3 Dans la zone de texte **[Initier la récupération lorsque l'espace inutilisé dépasse]** , tapez la quantité minimale d'espace disque inutilisé, en gigaoctets, qui doit être atteinte sur un disque du système d'exploitation de clone lié avant qu'ESXi démarre la récupération de l'espace sur ce disque.

   Par exemple : **2** Go.

   La valeur par défaut est 1 Go.

Suivant

Vous pouvez configurer des jours et des heures d'interruption durant lesquels la récupération d'espace disque et la régénération de View Storage Accelerator n'ont pas lieu. Reportez-vous à la section « Définir des heures d'interruption pour des opérations ESXi sur des postes de travail View », page 132.

Dans View Administrator, vous pouvez cliquer sur **[Inventaire] > [Postes de travail]** et sélectionner un poste de travail pour afficher l'heure de la dernière récupération d'espace et la dernière quantité d'espace récupéré sur le poste de travail.

Définir des heures d'interruption pour des opérations ESXi sur des postes de travail View

La régénération des fichiers condensés pour View Storage Accelerator et la récupération de l'espace disque de machine virtuelle peuvent utiliser des ressources ESXi. Pour vous assurer que des ressources ESXi sont dédiées à des tâches de premier plan lorsque cela est nécessaire, vous pouvez empêcher les hôtes ESXi d'exécuter ces opérations pendant des périodes de temps spécifiées certains jours.

Par exemple, vous pouvez spécifier une période d'interruption tous les matins du lundi au vendredi, lorsque les utilisateurs commencent à travailler. Des tempêtes de démarrage et des tempêtes d'E/S d'analyse antivirus ont lieu. Vous pouvez spécifier différentes heures d'interruption selon les jours.

La récupération d'espace disque et la régénération des fichiers condensés de View Storage Accelerator n'ont pas lieu lors des heures d'interruption que vous avez définies. Vous ne pouvez pas définir des heures d'interruption séparées pour chaque opération.

View permet aux fichiers condensés de View Storage Accelerator d'être créés pour les nouveaux postes de travail lors de l'étape d'approvisionnement, même lorsqu'une heure d'interruption est effective.

Prérequis

- Vérifiez que **[Activer View Storage Accelerator]**, **[Activer la récupération d'espace]** ou les deux fonctions sont sélectionnées pour vCenter Server.
- Vérifiez que **[Utiliser View Storage Accelerator]**, **[Récupérer l'espace disque de machine virtuelle]** ou les deux fonctions sont sélectionnées pour le pool de postes de travail.

Procédure

1. Sur la page Options de stockage avancées de l'assistant Ajouter un pool, allez à **[Durée d'interruption]** et cliquez sur **[Ajouter]**.

   Si vous modifiez un pool existant, cliquez sur l'onglet **[Options de stockage avancées]**.

2. Cochez les jours d'interruption et spécifiez les heures de début et de fin.

   Le sélecteur horaire utilise une horloge de 24 heures. Par exemple, 10:00 correspond à 10:00 a.m. et 22:00 à 10:00 p.m.

3. Cliquez sur **[OK]**.
4. Pour ajouter une autre période d'interruption, cliquez sur **[Ajouter]** et spécifiez une autre période.
5. Pour modifier ou supprimer une période d'interruption, sélectionnez la période dans la liste Heures d'interruption et cliquez sur **[Modifier]** ou **[Supprimer]**.

Maintien des postes de travail de clone lié approvisionnés et prêts lors d'opérations de View Composer

Si vos utilisateurs doivent pouvoir accéder à des postes de travail View à tout moment, vous devez maintenir un certain nombre de postes de travail qui restent approvisionnés et prêts à accepter les demandes de connexion de vos utilisateurs même lorsque des opérations de maintenance de View Composer sont en cours. Vous pouvez définir un nombre minimum de postes de travail approvisionnés et prêts pendant que View Composer actualise, recompose ou rééquilibre les machines virtuelles de clone lié dans un pool.

Lorsque vous spécifiez **[Nombre minimum de postes de travail prêts (approvisionnés) lors d'opérations de maintenance de View Composer]** , View Manager s'assure que le nombre spécifié de postes de travail reste approvisionné et prêt pendant que View Composer exécute l'opération. Vous pouvez spécifier le nombre minimum de postes de travail prêts lorsque vous créez ou modifiez un pool de clone lié.

Les recommandations suivantes s'appliquent à ce paramètre :

- Si vous utilisez un mode d'attribution de nom pour approvisionner des postes de travail et approvisionner des postes de travail à la demande, définissez le nombre de postes de travail prêts lors des opérations de View Composer sur une valeur inférieure à la valeur **[Nombre min. de postes de travail]** spécifiée. Si le nombre minimum était inférieur, votre pool pourrait finir avec un nombre total de postes de travail inférieur au nombre minimum que vous voulez maintenir approvisionnés et prêts lors des opérations de View Composer. Dans ce cas, les opérations de maintenance de View Composer ne pourraient pas avoir lieu.
- Si vous approvisionnez des postes de travail en spécifiant manuellement une liste de noms de poste de travail, ne réduisez pas la taille de pool totale (en supprimant les noms de poste de travail) à un nombre inférieur au nombre minimum de postes de travail prêts. Dans ce cas, les opérations de maintenance de View Composer ne pourraient pas avoir lieu.
- Si vous définissez un nombre minimum important de postes de travail prêts par rapport à la taille du pool, les opérations de maintenance de View Composer peuvent durer plus longtemps. Pendant que View Manager maintient le nombre minimum de postes de travail prêts lors d'une opération de maintenance, l'opération peut ne pas atteindre la limite de simultanéité spécifiée dans le paramètre **[Nombre max. d'opérations de maintenance View Composer simultanées]** .

  Par exemple, si un pool contient 20 postes de travail et que le nombre minimum de postes de travail prêts est 15, View Composer peut fonctionner sur 5 postes de travail maximum à la fois. Si la limite de simultanéité des opérations de maintenance de View Composer est de 12, elle n'est jamais atteinte.
- Le terme « prêt » s'applique à l'état de la machine virtuelle de clone lié, pas à l'état du poste de travail qui est affiché dans View Administrator. Une machine virtuelle est prête lorsqu'elle est approvisionnée et prête à être activée. L'état du poste de travail reflète la condition gérée par View du poste de travail. Par exemple, un poste de travail peut avoir l'état `Connecté`, `Déconnecté`, `Agent inaccessible)`, `Suppression`, etc.

Utiliser des comptes d'ordinateur Active Directory existants pour des clones liés

Lorsque vous créez ou modifiez un pool de postes de travail, vous pouvez configurer View Composer afin qu'il utilise des comptes d'ordinateur existants dans Active Directory pour les clones liés qui viennent d'être approvisionnés.

Par défaut, View Composer génère un nouveau compte d'ordinateur Active Directory pour chaque clone lié qu'il approvisionne. L'option **[Autoriser la réutilisation de comptes d'ordinateur pré-existants]** vous permet de contrôler les comptes d'ordinateur qui sont créés dans Active Directory en garantissant que View Composer utilise des comptes d'ordinateur AD existants.

Avec cette option activée, lorsqu'un clone lié est approvisionné, View Composer vérifie si un nom de compte d'ordinateur AD existant correspond au nom du poste de travail de clone lié. Si une correspondance existe, View Composer utilise le compte d'ordinateur AD existant. Si View Composer ne trouve pas de nom de compte d'ordinateur AD correspondant, il génère un nouveau compte d'ordinateur AD pour le clone lié.

Vous pouvez définir l'option **[Autoriser la réutilisation de comptes d'ordinateur pré-existants]** lorsque vous créez un nouveau pool de postes de travail ou modifiez un pool existant. Si vous modifiez un pool et définissez cette option, le paramètre affecte les postes de travail de clone lié qui sont approvisionnés dans le futur. Les clones liés qui sont déjà approvisionnés ne sont pas affectés.

Lorsque vous définissez l'option **[Autoriser la réutilisation de comptes d'ordinateur pré-existants]** , vous pouvez limiter les autorisations Active Directory affectées au compte d'utilisateur View Composer qui génère le pool de postes de travail. Seules les autorisations Active Directory suivantes sont requises :

- Contenu de la liste
- Lire toutes les propriétés
- Lire les autorisations
- Réinitialiser le mot de passe

Vous ne pouvez limiter les autorisations Active Directory que si vous êtes sûr que tous les postes de travail que vous prévoyez d'approvisionner ont des comptes d'ordinateur existants alloués dans Active Directory. View Composer génère un nouveau compte d'ordinateur AD si aucun nom correspondant n'est trouvé. Des autorisations supplémentaires, telles que Créer des objets ordinateur, sont requises pour créer de nouveaux comptes d'ordinateur. Pour voir une liste complète des autorisations requises pour le compte d'utilisateur View Composer, reportez-vous à la section « Créer un compte d'utilisateur pour View Composer », page 15.

Cette option ne peut pas être désactivée si View Composer utilise actuellement au moins un compte d'ordinateur AD existant.

Prérequis

Vérifiez que les comptes d'ordinateur existants sont situés dans le conteneur Active Directory que vous spécifiez avec le paramètre **[Conteneur Active Directory]** . Si les comptes existants se trouvent dans un conteneur différent, l'approvisionnement échoue pour les clones liés avec ces noms de compte et un message d'erreur indique que les comptes d'ordinateur existants existent déjà dans Active Directory.

Par exemple, si vous sélectionnez l'option **[Autoriser la réutilisation de comptes d'ordinateur pré-existants]** et que vous spécifiez que le **[Conteneur Active Directory]** est la valeur par défaut, **`CN=Computers`**, et si les comptes d'ordinateur existants se trouvent dans **`OU=mydesktops`**, l'approvisionnement échoue pour ces comptes.

Procédure

1 Dans Active Directory, créez les comptes d'ordinateur à utiliser pour les postes de travail de clone lié.

Par exemple : `desktop1, desktop2, desktop3`

Les noms de compte d'ordinateur doivent utiliser des entiers consécutifs afin qu'ils correspondent aux noms des postes de travail View qui sont générés lors de l'approvisionnement de poste de travail.

2 Dans View Administrator, créez un pool avec l'assistant Ajouter un pool ou modifiez le pool dans la boîte de dialogue Modifier le pool.

3 Sur la page ou l'onglet Paramètres d'approvisionnement, sélectionnez **[Utiliser un mode d'attribution de nom]** .

4 Dans la zone de texte Mode d'attribution de nom, tapez un nom de poste de travail qui correspond au nom du compte d'ordinateur Active Directory.

   Par exemple : `poste de travail`

   View ajoute des numéros uniques au modèle pour fournir un nom unique à chaque poste de travail.

   Par exemple : `desktop1, desktop2, desktop3`

5 Sur la page ou l'onglet Personnalisation client, sélectionnez l'option **[Autoriser la réutilisation de comptes d'ordinateur pré-existants]** .

Disques de données du poste de travail de clone lié

View Composer crée plusieurs disques de données pour stocker les composants d'un poste de travail de clone lié.

Disque du système d'exploitation

View Composer crée un disque du système d'exploitation pour chaque clone lié. Ce disque stocke les données du système dont le clone a besoin pour rester lié à l'image de base et pour fonctionner en tant que poste de travail unique.

Disque de données de configuration QuickPrep

View Composer crée un deuxième disque avec le disque du système d'exploitation. Le deuxième disque stocke les données de configuration QuickPrep et d'autres données liées au système d'exploitation qui doivent être conservées au cours d'opérations d'actualisation et de recomposition. Le disque est de petite taille, généralement aux alentours de 20 Mo. Ce disque est créé si vous utilisez QuickPrep ou Sysprep pour personnaliser le poste de travail.

Si vous configurez des disques persistants séparés de View Composer pour stocker des profils d'utilisateur, 3 disques sont associés à chaque clone lié : le disque du système d'exploitation, le deuxième disque de poste de travail et le disque persistant de View Composer.

Le deuxième disque de poste de travail est stocké sur le même magasin de données que le disque du système d'exploitation. Vous ne pouvez pas configurer ce disque.

Disque persistant de View Composer

Dans un pool d'affectation dédiée, vous pouvez configurer des disques persistants séparés de View Composer pour stocker des données de profil d'utilisateur Windows. Ce disque est facultatif.

Les disques persistants séparés vous permettent de conserver des données et des paramètres d'utilisateur. Les opérations d'actualisation, de recomposition et de rééquilibrage de View Composer n'affectent pas les disques persistants. Vous pouvez détacher un disque persistant d'un clone lié et l'attacher à un autre clone lié.

Si vous ne configurez pas de disques persistants séparés, le profil Windows est stocké sur le disque du système d'exploitation. Les données et les paramètres d'utilisateur sont supprimés au cours des opérations d'actualisation, de recomposition et de rééquilibrage.

Vous pouvez stocker des disques persistants sur le même magasin de données que le disque du système d'exploitation ou sur un magasin de données différent.

Disque de données supprimables

Lorsque vous créez un pool de clone lié, vous pouvez configurer un disque non persistant séparé pour stocker les fichiers d'échange et temporaires du système d'exploitation client qui sont générés au cours de sessions utilisateur. Vous devez spécifier la taille du disque en mégaoctets.

Ce disque est facultatif.

Lorsque le clone lié est mis hors tension, View Manager remplace le disque de données supprimables par une copie du disque d'origine que View Composer a créé avec le pool de clone lié. La taille des clones liés peut augmenter à mesure que les utilisateurs interagissent avec leurs postes de travail. L'utilisation de disques de données supprimables peut économiser de l'espace de stockage en ralentissant la croissance des clones liés.

Le disque de données supprimables est stocké sur le même magasin de données que le disque du système d'exploitation.

Pools de postes de travail manuels

Pour créer un pool de postes de travail manuel, View Manager approvisionne des postes de travail depuis des sources de postes de travail existantes. Vous sélectionnez une source de poste de travail distincte pour chaque poste de travail du pool.

View Manager peut utiliser plusieurs types de sources de postes de travail dans des pools manuels :

- des machines virtuelles gérées par vCenter Server ;
- des machines virtuelles exécutées sur VMware Server ou sur une autre plate-forme de virtualisation ;
- Ordinateurs physiques
- des PC HP lame.

Feuille de calcul pour créer un pool de postes de travail manuel

Lorsque vous créez un pool de postes de travail manuel, l'assistant Add Pool (Ajouter un pool) de View Administrator vous invite à configurer certaines options. Utilisez cette feuille de calcul pour préparer vos options de configuration avant de créer le pool.

Vous pouvez imprimer cette feuille de calcul et noter les valeurs que vous souhaitez spécifier quand vous exécutez l'assistant Add Pool (Ajouter un pool).

Remarque Dans un pool manuel, vous devez préparer chaque source de postes de travail à fournir un accès au poste de travail View. View Agent doit être installé et exécuté sur chaque source de postes de travail.

Tableau 5-13. Feuille de calcul : options de configuration pour créer un pool de postes de travail manuel

Option	Description	Indiquez votre valeur ici
User assignment (Affectation d'utilisateur)	Choisissez le type d'affectation d'utilisateur : ■ Dans un pool d'affectation dédiée, chaque utilisateur est affecté à un poste de travail. Les utilisateurs reçoivent le même poste de travail chaque fois qu'ils ouvrent une session. ■ Dans un pool d'affectation flottante, les utilisateurs reçoivent différents postes de travail chaque fois qu'ils ouvrent une session. Pour plus d'informations, reportez-vous à la section « Affectation d'utilisateur dans des pools de postes de travail », page 143.	
Desktop Sources (Sources de postes de travail)	Machines virtuelles ou ordinateurs physiques que vous voulez utiliser en tant que postes de travail View dans le pool. 1 Décidez du type de source de postes de travail que vous voulez utiliser. Vous pouvez utiliser des machines virtuelles gérées par vCenter Server ou des machines virtuelles, des ordinateurs physiques et des PC lame non gérés. 2 Préparez une liste des machines virtuelles vCenter Server ou des machines virtuelles, des ordinateurs physiques et des PC lame non gérés que vous voulez inclure dans le pool. Pour utiliser PCoIP avec des sources de postes de travail qui sont des machines virtuelles, des ordinateurs physiques ou des PC lame non gérés, vous devez utiliser un matériel Teradici.	
vCenter Server	vCenter Server qui gère les postes de travail. Cette option apparaît uniquement si les sources de postes de travail sont des machines virtuelles gérées par vCenter Server.	
Pool ID (ID de pool)	Nom de pool que les utilisateurs voient lorsqu'ils ouvrent une session et qui identifie le pool dans View Administrator. Si plusieurs serveurs vCenter Server sont exécutés dans votre environnement, assurez-vous qu'aucun autre serveur vCenter Server n'utilise le même ID de pool.	
Pool Settings (Paramètres de pool)	Paramètres qui déterminent l'état du poste de travail, l'état d'alimentation quand une machine virtuelle n'est pas utilisée, le protocole d'affichage, la qualité Adobe Flash, etc. Pour plus d'informations, reportez-vous à la section « Paramètres de poste de travail et de pool », page 151. Pour voir une liste des paramètres qui s'appliquent à des pools manuels, reportez-vous à la section « Paramètres de poste de travail pour des pools manuels », page 140.	

Créer un pool de postes de travail manuel

Vous pouvez créer un pool de postes de travail manuel qui approvisionne des postes de travail depuis des machines virtuelles, des ordinateurs physiques et des PC HP lame existants. Vous devez sélectionner les sources de postes de travail qui composent les postes de travail View dans le pool.

Pour les pools manuels avec des postes de travail gérés par vCenter Server, View Manager garantit qu'un poste de travail de rechange est activé afin que les utilisateurs puissent s'y connecter. Le poste de travail de rechange est activé quelle que soit la règle d'alimentation appliquée.

Prérequis

- Préparez les sources de postes de travail à fournir un accès au poste de travail View. Dans un pool manuel, vous devez préparer chaque source de postes de travail individuellement. View Agent doit être installé et exécuté sur chaque source de postes de travail.

  Pour préparer des machines virtuelles gérées par vCenter Server, reportez-vous au Chapitre 4, « Création et préparation de machines virtuelles », page 65.

  Pour préparer des machines virtuelles, des ordinateurs physiques et des PC lame non gérés, reportez-vous au Chapitre 3, « Préparation de sources de postes de travail non gérées », page 61.

- Collectez les informations de configuration que vous devez fournir pour créer le pool. Reportez-vous à la section « Feuille de calcul pour créer un pool de postes de travail manuel », page 136.

- Décidez comment configurer les paramètres d'alimentation, le protocole d'affichage, la qualité Adobe Flash et d'autres paramètres. Reportez-vous à la section « Paramètres de poste de travail et de pool », page 151.

Procédure

1 Dans View Administrator, cliquez sur **[Inventory (Inventaire)] > [Pools]** .

2 Cliquez sur **[Add (Ajouter)]** .

3 Sélectionnez **[Manual Pool (Pool manuel)]** .

4 Suivez les invites de l'assistant pour créer le pool.

  Utilisez les informations de configuration que vous avez collectées dans la feuille de calcul. Vous pouvez revenir directement à n'importe quelle page de l'assistant en cliquant sur le nom de page dans le volet de navigation.

Dans View Administrator, vous pouvez voir les postes de travail lorsqu'ils sont ajoutés au pool en cliquant sur **[Inventory (Inventaire)] > [Postes de travail]** .

Suivant

Autorisez les utilisateurs à accéder au pool. Reportez-vous à la section « Ajouter des autorisations à des pools de postes de travail », page 171.

Créer un pool manuel contenant un poste de travail

Vous pouvez créer un pool contenant un seul poste de travail quand un utilisateur requiert un poste de travail dédié unique, ou quand plusieurs utilisateurs doivent accéder à une application coûteuse avec une seule licence hôte à des heures différentes.

Vous pouvez approvisionner un poste de travail View individuel dans son propre pool en créant un pool de postes de travail manuel et en sélectionnant une source de postes de travail.

Pour imiter un ordinateur physique pouvant être partagé par plusieurs utilisateurs, spécifiez une affectation flottante pour les utilisateurs autorisés à accéder au pool.

Que vous configuriez le pool de poste de travail unique avec une affectation dédiée ou flottante, les opérations d'alimentation sont initiées par la gestion des sessions. La machine virtuelle est activée lorsqu'un utilisateur demande le poste de travail, et désactivée ou interrompue quand l'utilisateur ferme sa session.

Si vous configurez la règle **[Ensure desktops are always powered on (S'assurer que les postes de travail sont toujours activés)]** , la machine virtuelle reste activée. Si l'utilisateur éteint la machine virtuelle, elle redémarre immédiatement.

Prérequis

- Préparez la source de postes de travail à fournir un accès au poste de travail View. View Agent doit être installé et exécuté sur la source de postes de travail.

  Pour préparer une machine virtuelle gérée par vCenter Server, reportez-vous au Chapitre 4, « Création et préparation de machines virtuelles », page 65.

  Pour préparer une machine virtuelle, un ordinateur physique ou un PC lame non géré, reportez-vous au Chapitre 3, « Préparation de sources de postes de travail non gérées », page 61.

- Collectez les informations de configuration que vous devez fournir pour créer le pool manuel. Reportez-vous à la section « Feuille de calcul pour créer un pool de postes de travail manuel », page 136.

- Décidez comment configurer les paramètres d'alimentation, le protocole d'affichage, la qualité Adobe Flash et d'autres paramètres. Reportez-vous à la section « Paramètres de poste de travail et de pool », page 151.

Procédure

1 Dans View Administrator, cliquez sur **[Inventory (Inventaire)] > [Pools]** .

2 Cliquez sur **[Add (Ajouter)]** .

3 Sélectionnez **[Manual Pool (Pool manuel)]** .

4 Sélectionnez le type d'affectation d'utilisateur.

Option	Description
Dedicated Assignment (Affectation dédiée)	Le poste de travail est affecté à un utilisateur. Seul cet utilisateur peut ouvrir une session sur le poste de travail.
Floating Assignment (Affectation flottante)	Le poste de travail est partagé par tous les utilisateurs qui sont autorisés sur le pool. N'importe quel utilisateur autorisé peut ouvrir une session sur le poste de travail tant qu'un autre utilisateur n'y a pas ouvert de session.

5 Sur la page Add vCenter Virtual Machines (Ajouter des machines virtuelles vCenter) ou Add Machines (Ajouter des machines), sélectionnez la source de postes de travail de votre poste de travail.

6 Suivez les invites de l'assistant pour créer le pool.

  Utilisez les informations de configuration que vous avez collectées dans la feuille de calcul. Vous pouvez revenir directement à n'importe quelle page de l'assistant en cliquant sur le nom de page dans le volet de navigation.

Dans View Administrator, vous pouvez afficher le poste de travail lors du processus de création en cliquant sur **[Inventory (Inventaire)] > [Desktops (Postes de travail)]** .

Suivant

Autorisez les utilisateurs à accéder au pool. Reportez-vous à la section « Ajouter des autorisations à des pools de postes de travail », page 171.

Paramètres de poste de travail pour des pools manuels

Vous devez spécifier des paramètres de poste de travail et de pool lorsque vous configurez des pools manuels. Les paramètres ne s'appliquent pas à tous les types de pools manuels.

Tableau 5-14 répertorie les paramètres qui s'appliquent à des pools de postes de travail manuels qui sont configurés avec ces propriétés :

- des affectations d'utilisateur dédiées ;
- des affectations d'utilisateur flottantes ;
- des sources de postes de travail gérées (machines virtuelles vCenter Server) ;
- des sources de postes de travail non gérées.

Ces paramètres s'appliquent également à un pool manuel contenant un seul poste de travail.

Pour voir des descriptions de chaque paramètre de poste de travail, reportez-vous à la section « Paramètres de poste de travail et de pool », page 151.

Tableau 5-14. Paramètres des pools de postes de travail manuels

Paramètre	Pool géré manuel, affectation dédiée	Pool géré manuel, affectation flottante	Pool non géré manuel, affectation dédiée	Pool non géré manuel, affectation flottante
État	Oui	Oui	Oui	Oui
Restrictions de Serveur de connexion	Oui	Oui	Oui	Oui
Règle d'alimentation de poste de travail distant	Oui	Oui		
Fermeture de session automatique après la déconnexion	Oui	Oui	Oui	Oui
Autoriser les utilisateurs à réinitialiser leur poste de travail	Oui	Oui		
Autoriser plusieurs sessions par utilisateur		Oui		Oui
Protocole d'affichage par défaut	Oui	Oui	Oui Pour utiliser PCoIP avec une source de postes de travail non gérée par vCenter Server, vous devez installer le matériel Teradici sur la source de postes de travail.	Oui Pour utiliser PCoIP avec une source de postes de travail non gérée par vCenter Server, vous devez installer le matériel Teradici sur la source de postes de travail.
Autoriser les utilisateurs à choisir un protocole	Oui	Oui	Oui	Oui

Tableau 5-14. Paramètres des pools de postes de travail manuels (suite)

Paramètre	Pool géré manuel, affectation dédiée	Pool géré manuel, affectation flottante	Pool non géré manuel, affectation dédiée	Pool non géré manuel, affectation flottante
Convertisseur 3D	Oui	Oui		
Nombre max. d'écrans	Oui	Oui		
Résolution max. d'un écran	Oui	Oui		
Qualité Adobe Flash	Oui	Oui	Oui	Oui
Limitation d'Adobe Flash	Oui	Oui	Oui	Oui

Pools Microsoft Terminal Services

Vous pouvez utiliser des serveurs Microsoft Terminal Server pour fournir des sessions Terminal Services en tant que postes de travail à des clients View. View Manager gère les sessions Terminal Services de la même façon qu'il gère d'autres postes de travail View.

Un pool Terminal Services peut contenir plusieurs sources de postes de travail servies par un ou plusieurs serveurs Terminal Server. Une source de postes de travail Terminal Server peut livrer plusieurs postes de travail View.

View Manager fournit un équilibrage de charge aux serveurs Terminal Server dans un pool, en dirigeant les demandes de connexion au serveur Terminal Server ayant le moins de sessions actives.

Vous autorisez l'accès d'un pool Terminal Services complet à des utilisateurs ou des groupes d'utilisateurs.

Vous devez déployer une solution de profil itinérant pour propager des paramètres d'utilisateur et des données au poste de travail auquel l'utilisateur accède actuellement.

Remarque Les pools Terminal Services ne prennent en charge que le protocole d'affichage RDP.

Créer un pool Microsoft Terminal Services

Vous pouvez créer un pool Microsoft Terminal Services qui approvisionne des postes de travail depuis des sources de postes de travail Terminal Server. Vous devez sélectionner les sources de postes de travail qui composent les postes de travail View dans le pool.

Prérequis

- Préparez les sources de postes de travail Terminal Server à fournir un accès au poste de travail View. View Agent doit être installé et exécuté sur chaque source de postes de travail. Reportez-vous à la section Chapitre 3, « Préparation de sources de postes de travail non gérées », page 61.
- Faites une liste des sources de postes de travail Terminal Server que vous voulez inclure dans le pool.
- Décidez comment configurer les paramètres de poste de travail. Reportez-vous à la section « Paramètres de poste de travail pour des pools Microsoft Terminal Services », page 142. Pour voir des descriptions de chaque paramètre de poste de travail, reportez-vous à la section « Paramètres de poste de travail et de pool », page 151.
- Fournissez un ID de pool que les utilisateurs voient lorsqu'ils ouvrent une session et qui identifie le pool dans View Administrator. Si plusieurs serveurs vCenter Server sont exécutés dans votre environnement, assurez-vous qu'aucun autre serveur vCenter Server n'utilise le même ID de pool.

Procédure

1 Dans View Administrator, cliquez sur **[Inventory (Inventaire)] > [Pools]** .

2 Cliquez sur **[Add (Ajouter)]** .

3 Sélectionnez **[Terminal Services Pool (Pool Terminal Services)]** .

4 Suivez les invites de l'assistant pour créer le pool.

Utilisez les informations de configuration que vous avez collectées dans la feuille de calcul. Vous pouvez revenir directement à n'importe quelle page de l'assistant en cliquant sur le nom de page dans le volet de navigation.

Dans View Administrator, vous pouvez voir les postes de travail lorsqu'ils sont ajoutés au pool en cliquant sur **[Inventory (Inventaire)] > [Postes de travail]** .

Suivant

Autorisez les utilisateurs à accéder au pool. Reportez-vous à la section « Ajouter des autorisations à des pools de postes de travail », page 171.

Paramètres de poste de travail pour des pools Microsoft Terminal Services

Vous devez spécifier des paramètres de poste de travail et de pool lorsque vous configurez des pools Microsoft Terminal Services. Les paramètres ne s'appliquent pas à tous les types de pools Terminal Services.

Tableau 5-15 répertorie les paramètres qui s'appliquent à des pools Terminal Services.

Pour voir des descriptions de chaque paramètre de poste de travail, reportez-vous à la section « Paramètres de poste de travail et de pool », page 151.

Tableau 5-15. Paramètres des pools Terminal Services

Paramètre	Pool Microsoft Terminal Services
State (État)	Oui
Connection Server restrictions (Restrictions de Connection Server)	Oui
Automatic logoff after disconnect (Fermeture de session automatique après la déconnexion)	Oui
Default display protocol (Protocole d'affichage par défaut)	RDP est le seul protocole d'affichage pris en charge pour les pools Terminal Services.
Adobe Flash quality (Qualité Adobe Flash)	Oui
Adobe Flash throttling (Limitation d'Adobe Flash)	Oui

Configurer la limitation d'Adobe Flash avec Internet Explorer dans des sessions Terminal Services

Pour s'assurer que la limitation d'Adobe Flash fonctionne avec Internet Explorer dans des sessions Terminal Services, les utilisateurs doivent activer des extensions tierce partie du navigateur.

Procédure

1 Démarrez View Client et ouvrez une session sur le poste de travail d'un utilisateur.

2 Dans Internet Explorer, cliquez sur **[Tools (Outils)] > [Internet Options (Options Internet)]** .

3 Cliquez sur l'onglet **[Advanced (Avancé)]** , sélectionnez **[Enable third-party browser extensions (Activer les extensions tierce partie du navigateur)]** , puis cliquez sur **[OK]** .

4 Redémarrez Internet Explorer.

Approvisionnement de pools de postes de travail

Lorsque vous créez un pool de postes de travail, vous sélectionnez des options de configuration qui déterminent la façon dont le pool est géré et comment les utilisateurs interagissent avec les postes de travail.

- Affectation d'utilisateur dans des pools de postes de travail page 143

  Vous pouvez configurer un pool de postes de travail pour que les utilisateurs aient des affectations dédiées ou flottantes sur les postes de travail du pool. Vous devez choisir une affectation d'utilisateur pour les pools automatisés qui contiennent des machines virtuelles complètes, des pools de clone lié automatisés et des pools manuels.

- Nommer des postes de travail manuellement ou fournir un mode d'attribution de nom page 144

  Vous pouvez approvisionner les postes de travail dans un pool automatisé en spécifiant manuellement une liste de noms de poste de travail ou en fournissant un mode d'attribution de nom et le nombre de postes de travail que vous voulez dans le pool. Ces deux approches offrent des avantages différents.

- Personnalisation manuelle de postes de travail page 150

  Après avoir créé un pool automatisé, vous pouvez personnaliser des postes de travail particuliers sans réaffecter la propriété. En démarrant les postes de travail en mode de maintenance, vous pouvez modifier et tester les postes de travail avant de les libérer pour leurs utilisateurs affectés ou les rendre disponibles à tous les utilisateurs autorisés dans le pool.

- Paramètres de poste de travail et de pool page 151

  Vous devez spécifier des paramètres de poste de travail et de pool lorsque vous configurez des pools automatisés contenant des machines virtuelles complètes, des pools de postes de travail de clone lié, des pools de postes de travail manuels et des pools Microsoft Terminal Services. Les paramètres ne s'appliquent pas à tous les types de pools de postes de travail.

- Configuration du rendu 3D sur des postes de travail Windows 7 ou supérieur page 156

  Lorsque vous créez ou modifiez un pool de postes de travail Windows 7 ou supérieur, vous pouvez configurer un rendu graphique 3D pour vos postes de travail. Les postes de travail peuvent bénéficier de vSGA (Virtual Shared Graphics Acceleration), une fonction de vSphere qui utilise des cartes graphiques physiques installées sur les hôtes ESXi et qui gère les ressources de processeur graphique parmi les postes de travail.

- Empêcher l'accès à des postes de travail View via RDP page 160

  Dans certains environnements View, interdire l'accès à des postes de travail View via le protocole d'affichage RDP est une priorité. Vous pouvez empêcher des utilisateurs et des administrateurs d'utiliser RDP pour accéder à des postes de travail View en configurant des paramètres de pool et un paramètre de stratégie de groupe.

Affectation d'utilisateur dans des pools de postes de travail

Vous pouvez configurer un pool de postes de travail pour que les utilisateurs aient des affectations dédiées ou flottantes sur les postes de travail du pool. Vous devez choisir une affectation d'utilisateur pour les pools automatisés qui contiennent des machines virtuelles complètes, des pools de clone lié automatisés et des pools manuels.

Avec une affectation dédiée, View Manager affecte chaque utilisateur autorisé à un poste de travail du pool. Lorsqu'un utilisateur se connecte au pool, l'utilisateur ouvre toujours une session sur le même poste de travail. Les paramètres et les données de l'utilisateur sont enregistrés entre les sessions. Aucun autre utilisateur dans le pool ne peut accéder au poste de travail.

Avec une affectation flottante, View Manager affecte dynamiquement des postes de travail du pool à des utilisateurs autorisés. Les utilisateurs se connectent à un poste de travail différent chaque fois qu'ils ouvrent une session. Lorsqu'un utilisateur ferme sa session, le poste de travail est renvoyé au pool.

Vous pouvez configurer des postes de travail d'affectation flottante à supprimer quand des utilisateurs ferment leur session. La suppression automatique vous permet de ne conserver que les machines virtuelles dont vous avez besoin en même temps. Vous ne pouvez utiliser la suppression automatique que dans des pools automatisés que vous approvisionnez avec un mode d'attribution de nom de poste de travail et un nombre total de postes de travail.

Les postes de travail d'affectation flottante vous permettent de réduire les coûts de licence logicielle.

Nommer des postes de travail manuellement ou fournir un mode d'attribution de nom

Vous pouvez approvisionner les postes de travail dans un pool automatisé en spécifiant manuellement une liste de noms de poste de travail ou en fournissant un mode d'attribution de nom et le nombre de postes de travail que vous voulez dans le pool. Ces deux approches offrent des avantages différents.

Si vous nommez des postes de travail en spécifiant une liste, vous pouvez utiliser le schéma de nommage de votre entreprise, et vous pouvez associer chaque nom de poste de travail à un utilisateur.

Si vous fournissez un mode d'attribution de nom, View Manager peut créer et affecter dynamiquement des postes de travail à mesure que les utilisateurs en ont besoin.

Vous devez utiliser l'une de ces méthodes de nommage pour approvisionner des pools automatisés qui contiennent des machines virtuelles complètes ou des clones liés.

Tableau 5-16 compare les deux méthodes de nommage, en montrant comment chaque méthode affecte la façon dont vous créez et administrez un pool de postes de travail.

Tableau 5-16. Nommer des postes de travail manuellement ou fournir un mode d'attribution de nom de poste de travail

Fonction	En fournissant un mode d'attribution de nom de poste de travail	En nommant des postes de travail manuellement
Noms de poste de travail	View Manager génère des noms de poste de travail. Vous fournissez un mode d'attribution de nom. View Manager ajoute un numéro unique pour identifier chaque poste de travail. Pour plus d'informations, reportez-vous à la section « Utilisation d'un mode d'attribution de nom pour des pools de postes de travail automatisés », page 147.	Vous spécifiez une liste de noms de poste de travail. Dans un pool d'affectation dédiée, vous pouvez coupler des utilisateurs avec des postes de travail en listant des noms d'utilisateur avec les noms de poste de travail. Pour plus d'informations, reportez-vous à la section « Spécifier une liste de noms de poste de travail », page 146.
Taille de pool	Vous spécifiez un nombre maximum de postes de travail.	Votre liste de noms de poste de travail détermine le nombre de postes de travail.
Pour ajouter des postes de travail au pool	Vous pouvez augmenter la taille de pool maximale.	Vous pouvez ajouter des noms de poste de travail à la liste. Pour plus d'informations, reportez-vous à la section « Ajouter des postes de travail à un pool automatisé approvisionné par une liste de noms », page 308.

Tableau 5-16. Nommer des postes de travail manuellement ou fournir un mode d'attribution de nom de poste de travail (suite)

Fonction	En fournissant un mode d'attribution de nom de poste de travail	En nommant des postes de travail manuellement
Approvisionnement à la demande	Disponible. View Manager crée et provisionne dynamiquement le nombre défini de postes de travail minimal et de rechange lorsque les utilisateurs ouvrent une session pour la première fois ou lorsque vous affectez des postes de travail aux utilisateurs. View Manager peut également créer et approvisionner tous les postes de travail lorsque vous créez le pool.	Non disponible. View Manager crée et approvisionne tous les postes de travail que vous spécifiez dans votre liste lorsque le pool est créé.
Personnalisation initiale	Disponible. Lorsqu'un poste de travail est approvisionné, View Manager peut exécuter une spécification de personnalisation que vous sélectionnez.	Disponible. Lorsqu'un poste de travail est approvisionné, View Manager peut exécuter une spécification de personnalisation que vous sélectionnez.
Personnalisation manuelle de postes de travail dédiés	Pour personnaliser des postes de travail et renvoyer l'accès au poste de travail à vos utilisateurs, vous devez supprimer et réaffecter la propriété de chaque poste de travail. En fonction de l'affectation ou non de postes de travail lors de la première ouverture de session, il se peut que vous deviez effectuer ces étapes deux fois. Vous ne pouvez pas démarrer des postes de travail en mode de maintenance. Après la création du pool, vous pouvez mettre manuellement les postes de travail en mode de maintenance.	Vous pouvez personnaliser et tester des postes de travail sans avoir à réaffecter la propriété. Lorsque vous créez le pool, vous pouvez démarrer tous les postes de travail en mode de maintenance pour empêcher les utilisateurs d'y accéder. Vous pouvez personnaliser les postes de travail et quitter le mode de maintenance pour renvoyer l'accès à vos utilisateurs. Pour plus d'informations, reportez-vous à la section « Personnalisation manuelle de postes de travail », page 150.
Taille de pool dynamique ou fixe	Dynamique. Si vous supprimez une affectation d'utilisateur d'un poste de travail dans un pool d'affectation dédiée, le poste de travail est renvoyé au pool contenant les postes de travail disponibles. Si vous choisissez de supprimer des postes de travail à la fermeture de session dans un pool d'affectation flottante, la taille de pool peut croître ou diminuer en fonction du nombre de sessions utilisateur actives.	Fixe. Le pool contient le nombre de postes de travail que vous indiquez dans la liste de noms de poste de travail. Vous ne pouvez pas sélectionner le paramètre **[Delete desktop on logoff (Supprimer le poste de travail à la fermeture de session)]** si vous nommez les postes de travail manuellement.

Tableau 5-16. Nommer des postes de travail manuellement ou fournir un mode d'attribution de nom de poste de travail (suite)

Fonction	En fournissant un mode d'attribution de nom de poste de travail	En nommant des postes de travail manuellement
Postes de travail de rechange	Vous pouvez spécifier un nombre de postes de travail de rechange que View Manager maintient activés pour les nouveaux utilisateurs. View Manager crée de nouveaux postes de travail pour conserver le nombre spécifié. View Manager cesse de créer des postes de travail de rechange lorsqu'il atteint la taille de pool maximale. View Manager maintient les postes de travail de rechange activés même quand la règle d'alimentation du pool est **[Power off (Désactiver)]** ou **[Suspend (Interrompre)]** , ou quand vous ne définissez aucune règle d'alimentation.	Vous pouvez spécifier un nombre de postes de travail de rechange que View Manager maintient activés pour les nouveaux utilisateurs. View Manager ne crée pas de nouveaux postes de travail de rechange pour conserver le nombre spécifié. View Manager maintient les postes de travail de rechange activés même quand la règle d'alimentation du pool est **[Power off (Désactiver)]** ou **[Suspend (Interrompre)]** , ou quand vous ne définissez aucune règle d'alimentation.
User assignment (Affectation d'utilisateur)	Vous pouvez utiliser un mode d'attribution de nom pour des pools d'affectation dédiée et flottante.	Vous pouvez spécifier des noms de poste de travail pour des pools d'affectation dédiée et flottante. **Remarque** Dans un pool d'affectation flottante, vous ne pouvez pas associer des noms d'utilisateur à des noms de poste de travail. Les postes de travail ne sont pas dédiés aux utilisateurs associés. Dans un pool d'affectation flottante, tous les postes de travail qui ne sont pas actuellement utilisés restent accessibles à tout utilisateur ouvrant une session.

Spécifier une liste de noms de poste de travail

Vous pouvez approvisionner un pool de postes de travail automatisé en spécifiant manuellement une liste de noms de poste de travail. Cette méthode de nommage vous permet d'utiliser les conventions de dénomination de votre entreprise pour identifier les postes de travail dans un pool.

Lorsque vous spécifiez explicitement des noms de poste de travail, les utilisateurs peuvent voir des noms familiers basés sur l'organisation de leur entreprise quand ils ouvrent une session sur leurs postes de travail.

Suivez ces recommandations pour spécifier manuellement des noms de poste de travail :

- Saisissez chaque nom de poste de travail sur une ligne séparée.
- Un nom de poste de travail peut contenir 15 caractères alphanumériques maximum.
- Vous pouvez ajouter un nom d'utilisateur à chaque entrée de poste de travail. Utilisez une virgule pour séparer le nom d'utilisateur du nom de poste de travail.

Dans cet exemple, deux postes de travail sont spécifiés. Le deuxième poste de travail est associé à un utilisateur :

```
Desktop-001
Desktop-002,abccorp.com/jdoe
```

Remarque Dans un pool d'affectation flottante, vous ne pouvez pas associer des noms d'utilisateur à des noms de poste de travail. Les postes de travail ne sont pas dédiés aux utilisateurs associés. Dans un pool d'affectation flottante, tous les postes de travail qui ne sont pas actuellement utilisés restent accessibles à tout utilisateur ouvrant une session.

Prérequis

Assurez-vous que chaque nom de poste de travail est unique. Vous ne pouvez pas utiliser les noms de machines virtuelles existantes dans vCenter Server.

Procédure

1 Créez un fichier texte contenant la liste des noms de poste de travail.

Si vous prévoyez de créer un pool avec seulement quelques postes de travail, vous pouvez saisir les noms de poste de travail directement dans l'assistant Add Pool (Ajouter un pool). Vous n'avez pas à créer un fichier texte séparé.

2 Dans View Administrator, démarrez l'assistant Add Pool (Ajouter un pool) pour commencer la création d'un pool de postes de travail automatisé.

3 Sur la page Provisioning Settings (Paramètres d'approvisionnement), sélectionnez **[Specify names manually (Spécifier des noms manuellement)]** et cliquez sur **[Enter names (Saisir des noms)]** .

4 Copiez votre liste de noms de poste de travail sur la page Enter Desktop Names (Saisir des noms de poste de travail) et cliquez sur **[Next (Suivant)]** .

L'assistant Enter Desktop Names (Saisir des noms de poste de travail) affiche la liste des postes de travail et indique les erreurs de validation avec un point d'exclamation (**[!]**) rouge.

5 Corrigez les noms de poste de travail non valides.

a Placez votre curseur sur un nom non valide pour afficher le message d'erreur lié en bas de la page.

b Cliquez sur **[Back (Précédent)]** .

c Modifiez les noms incorrects et cliquez sur **[Next (Suivant)]** .

6 Cliquez sur **[Finish (Terminer)]** .

7 (Facultatif) Sélectionnez **[Start desktops in maintenance mode (Démarrer des postes de travail en mode de maintenance)]** .

Cette option vous permet de personnaliser les postes de travail avant que les utilisateurs puissent ouvrir une session et les utiliser.

8 Suivez les invites de l'assistant pour terminer la création du pool de postes de travail.

View Manager crée un poste de travail pour chaque nom dans la liste. Quand une entrée inclut un nom de poste de travail et un nom d'utilisateur, View Manager affecte le poste de travail à cet utilisateur.

Après la création du pool, vous pouvez ajouter des postes de travail en important un autre fichier de liste contenant des noms de poste de travail et des utilisateurs supplémentaires.

Utilisation d'un mode d'attribution de nom pour des pools de postes de travail automatisés

Vous pouvez approvisionner les postes de travail dans un pool en fournissant un mode d'attribution de nom et le nombre total de postes de travail que vous voulez dans le pool. Par défaut, View Manager utilise votre mode comme préfixe dans tous les noms de poste de travail et ajoute un numéro unique pour identifier chaque poste de travail.

Longueur du mode d'attribution de nom dans un nom de poste de travail

Les noms de poste de travail ont une limite de 15 caractères, y compris votre mode d'attribution de nom et le numéro généré automatiquement.

Tableau 5-17. Longueur maximale du mode d'attribution de nom dans un nom de poste de travail

Si vous définissez ce nombre de postes de travail dans le pool	Longueur de préfixe maximale
1-99	13 caractères
100-999	12 caractères
1 000 ou plus	11 caractères

Les noms contenant des jetons de longueur fixe ont des limites de longueur différentes. Pour plus d'informations sur la configuration de connexions directes, reportez-vous à la section « Longueur du mode d'attribution de nom quand vous utilisez un jeton de longueur fixe », page 148.

Utilisation d'un jeton dans un nom de poste de travail

Vous pouvez placer le numéro généré automatiquement n'importe où dans le nom en utilisant un jeton. Lorsque vous saisissez le nom de pool, saisissez **n** entre accolades pour désigner le jeton.

Par exemple : **amber-{n}-desktop**

Lorsque View Manager crée un poste de travail, View Manager remplace **{n}** par un numéro unique.

Vous pouvez générer un jeton de longueur fixe en saisissant **{n:fixed=*number of digits*}**.

View Manager remplace le jeton par des numéros contenant le nombre spécifié de chiffres.

Par exemple, si vous saisissez **amber-{n:fixed=3}**, View Manager remplace **{n:fixed=3}** par un nombre à trois chiffres et crée ces noms de poste de travail : **amber-001**, **amber-002**, **amber-003**, etc.

Longueur du mode d'attribution de nom quand vous utilisez un jeton de longueur fixe

Les noms qui contiennent des jetons de longueur fixe ont une limite de 15 caractères, y compris votre mode d'attribution de nom et le nombre de chiffres dans le jeton.

Tableau 5-18. Longueur maximale du mode d'attribution de nom quand vous utilisez un jeton de longueur fixe

Jeton de longueur fixe	Longueur maximale du mode d'attribution de nom
{n:fixed=1}	14 caractères
{n:fixed=2}	13 caractères
{n:fixed=3}	12 caractères

Exemple d'attribution de nom de poste de travail

Cet exemple montre comment créer deux pools de postes de travail automatisés qui utilisent les mêmes noms de poste de travail mais différents jeux de numéros. Les stratégies utilisées dans cet exemple atteignent un objectif d'utilisateur spécifique et montrent la flexibilité des méthodes de nommage de poste de travail.

L'objectif est de créer 2 pools avec la même convention de dénomination, telle que VDIABC-*XX*, où *XX* représente un numéro. Chaque pool a un jeu différent de numéros séquentiels. Par exemple, le premier pool peut contenir les postes de travail VDIABC-01 à VDIABC-10. Le deuxième pool contient les postes de travail VDIABC-11 à VDIABC-20.

Vous pouvez utiliser l'une des méthodes d'attribution de nom de poste de travail pour atteindre cet objectif.

- Pour créer des jeux fixes de postes de travail simultanément, spécifiez manuellement des noms de poste de travail.
- Pour créer des postes de travail dynamiquement lorsque des utilisateurs ouvrent une session pour la première fois, fournissez un mode d'attribution de nom et utilisez un jeton pour désigner les numéros séquentiels.

Spécification manuelle des noms

1 Préparez un fichier texte pour le premier pool contenant une liste de noms de poste de travail de VDIABC-01 à VDIABC-10.

2 Dans View Administrator, créez le pool et spécifiez les noms de poste de travail manuellement.

3 Cliquez sur **[Enter Names (Saisir des noms)]** et copiez votre liste dans la zone de liste **[Enter Desktop Names (Saisir des noms de poste de travail)]** .

4 Répétez ces étapes pour le deuxième pool, en utilisant les noms VDIABC-11 à VDIABC-20.

Pour plus d'informations, reportez-vous à la section « Spécifier une liste de noms de poste de travail », page 146.

Vous pouvez ajouter des postes de travail à chaque pool après sa création. Par exemple, vous pouvez ajouter des postes de travail VDIABC-21 à VDIABC-30 au premier pool et VDIABC-31 à VDIABC-40 au deuxième pool. Reportez-vous à la section « Ajouter des postes de travail à un pool automatisé approvisionné par une liste de noms », page 308.

Fournir un mode d'attribution de nom avec un jeton

1 Dans View Administrator, créez le premier pool et utilisez un mode d'attribution de nom pour approvisionner les noms de poste de travail.

2 Dans la zone de texte d'attribution de nom, saisissez **`VDIABC-0{n}`**.

3 Limitez la taille maximale du pool à 9.

4 Répétez ces étapes pour le deuxième pool, mais dans la zone de texte d'attribution de nom, saisissez **`VDIABC-1{n}`**.

Le premier pool contient les postes de travail VDIABC-01 à VDIABC-09. Le deuxième pool contient les postes de travail VDIABC-11 à VDIABC-19.

Vous pouvez également configurer les pools pour qu'ils contiennent 99 postes de travail maximum chacun en utilisant un jeton de longueur fixe à 2 chiffres :

- Pour le premier pool, saisissez **`VDIABC-0{n:fixed=2}`**.
- Pour le deuxième pool, saisissez **`VDIABC-1{n:fixed=2}`**.

Limitez la taille maximale de chaque pool à 99. Cette configuration produit des postes de travail contenant un mode d'attribution de nom séquentiel à 3 chiffres.

First pool:

```
VDIABC-001
VDIABC-002
VDIABC-003
```

Second pool:

```
VDIABC-101
VDIABC-102
VDIABC-103
```

Pour plus d'informations sur les modes d'attribution de nom et les jetons, reportez-vous à la section « Utilisation d'un mode d'attribution de nom pour des pools de postes de travail automatisés », page 147.

Personnalisation manuelle de postes de travail

Après avoir créé un pool automatisé, vous pouvez personnaliser des postes de travail particuliers sans réaffecter la propriété. En démarrant les postes de travail en mode de maintenance, vous pouvez modifier et tester les postes de travail avant de les libérer pour leurs utilisateurs affectés ou les rendre disponibles à tous les utilisateurs autorisés dans le pool.

- Personnalisation de postes de travail en mode de maintenance page 150

  Le mode de maintenance empêche les utilisateurs d'accéder à leurs postes de travail. Si vous démarrez des postes de travail en mode de maintenance, View Manager place chacun d'eux en mode de maintenance lorsque le poste de travail est créé.

- Personnaliser des postes de travail individuels page 150

  Vous pouvez personnaliser des postes de travail individuels après avoir créé un pool en démarrant les postes de travail en mode de maintenance.

Personnalisation de postes de travail en mode de maintenance

Le mode de maintenance empêche les utilisateurs d'accéder à leurs postes de travail. Si vous démarrez des postes de travail en mode de maintenance, View Manager place chacun d'eux en mode de maintenance lorsque le poste de travail est créé.

Dans un pool d'affectation dédiée, vous pouvez utiliser le mode de maintenance pour ouvrir une session sur un poste de travail sans avoir à réaffecter la propriété à votre propre compte d'administrateur. Lorsque vous avez terminé la personnalisation, vous n'avez pas à renvoyer la propriété à l'utilisateur affecté au poste de travail.

Dans un pool d'affectation flottante, vous pouvez tester des postes de travail en mode de maintenance avant de laisser des utilisateurs ouvrir leurs sessions.

Pour effectuer la même personnalisation sur tous les postes de travail dans un pool automatisé, personnalisez la machine virtuelle que vous préparez en tant que modèle ou parent. View Manager déploie votre personnalisation sur tous les postes de travail. Lorsque vous créez le pool, vous pouvez également utiliser une spécification de personnalisation Sysprep pour configurer tous les postes de travail avec des paramètres de licence, d'association de domaine, de protocole DHCP et d'autres propriétés informatiques.

Remarque Vous pouvez démarrer des postes de travail en mode de maintenance si vous spécifiez manuellement des noms de poste de travail pour le pool, et non si vous nommez des postes de travail en fournissant un mode d'attribution de nom.

Personnaliser des postes de travail individuels

Vous pouvez personnaliser des postes de travail individuels après avoir créé un pool en démarrant les postes de travail en mode de maintenance.

Procédure

1. Dans View Administrator, commencez par créer un pool de postes de travail automatisé en démarrant l'assistant Add Pool (Ajouter un pool).
2. Sur la page Provisioning Settings (Paramètres d'approvisionnement), sélectionnez **[Specify names manually (Spécifier des noms manuellement)]** .
3. Sélectionnez **[Start desktops in maintenance mode (Démarrer des postes de travail en mode de maintenance)]** .
4. Effectuez l'assistant Add Pool (Ajouter un pool) pour finir la création du pool de postes de travail.

5 Dans vCenter Server, ouvrez une session, personnalisez et testez les machines virtuelles de poste de travail individuelles.

Vous pouvez personnaliser les postes de travail manuellement ou en utilisant un logiciel de gestion des systèmes Windows standard comme Altiris, SMS, LanDesk ou BMC.

6 Dans View Administrator, sélectionnez le pool de postes de travail.

7 Utilisez l'outil de filtrage pour sélectionner des postes de travail à libérer pour les utilisateurs.

8 Cliquez sur **[Plus de commandes] > [Quitter le mode de maintenance]** .

Suivant

Informez vos utilisateurs qu'ils peuvent ouvrir une session sur leurs postes de travail.

Paramètres de poste de travail et de pool

Vous devez spécifier des paramètres de poste de travail et de pool lorsque vous configurez des pools automatisés contenant des machines virtuelles complètes, des pools de postes de travail de clone lié, des pools de postes de travail manuels et des pools Microsoft Terminal Services. Les paramètres ne s'appliquent pas à tous les types de pools de postes de travail.

Tableau 5-19. Descriptions des paramètres de poste de travail et de pool

Paramètre	Options
État	■ **[Activé]** . Une fois créé, le pool de postes de travail est activé et prêt pour une utilisation immédiate. ■ **[Désactivé]** . Une fois créé, le pool de postes de travail est désactivé et ne peut pas être utilisé. L'approvisionnement est arrêté pour le pool. Il s'agit d'un paramètre approprié si vous voulez réaliser des activités de post-déploiement comme des tests ou d'autres formes de maintenance de ligne de base. Lorsque cet état est effectif, les postes de travail distants sont indisponibles. En outre, les sessions de poste de travail local actives sont interrompues et les postes de travail locaux sont indisponibles.
Restrictions de Serveur de connexion	■ **[Aucune]** . Le pool de postes de travail peut être accédé par n'importe quelle instance de Serveur de connexion View. ■ **[Avec balises]** . Sélectionnez une ou plusieurs balises Serveur de connexion View pour rendre le pool de postes de travail accessible uniquement aux instances de Serveur de connexion View qui comportent ces balises. Vous pouvez utiliser les cases à cocher pour sélectionner plusieurs balises. Si vous prévoyez de fournir l'accès à vos postes de travail via Horizon Workspace, et si vous configurez des restrictions de Serveur de connexion View, Horizon User Portal peut afficher les postes de travail aux utilisateurs lorsque ces postes de travail sont en fait limités. Les utilisateurs Horizon ne pourront pas lancer ces postes de travail.

Tableau 5-19. Descriptions des paramètres de poste de travail et de pool (suite)

Paramètre	Options
Règle d'alimentation de poste de travail distant	Détermine comment une machine virtuelle se comporte quand un utilisateur ferme sa session sur le poste de travail associé. Pour voir des descriptions des options de règle d'alimentation, reportez-vous à la section « Règles d'alimentation pour des pools de postes de travail », page 161. Pour plus d'informations sur la façon dont les règles d'alimentation affectent les pools automatisés, reportez-vous à la section « Définition de règles d'alimentation pour des pools de postes de travail », page 161.
Fermeture de session automatique après la déconnexion	■ **[Immédiatement]** . La session des utilisateurs est fermée dès que ceux-ci se déconnectent. ■ **[Jamais]** . La session des utilisateurs n'est jamais fermée. ■ **[Après]** . Durée après laquelle la session des utilisateurs est fermée lorsque ceux-ci se déconnectent. Saisissez la durée en minutes. L'heure de fermeture de session s'applique aux déconnexions futures. Si un utilisateur a déjà fermé une session de poste de travail lorsque vous définissez une heure de fermeture de session, la durée de fermeture pour cet utilisateur démarre au moment où vous définissez l'heure de fermeture de session, pas lorsque l'utilisateur a fermé sa session. Par exemple, si vous définissez cette valeur sur 5 minutes, et qu'une session a été fermée 10 minutes plus tôt, View fermera cette session 5 minutes après que vous avez défini la valeur.
Autoriser les utilisateurs à réinitialiser leurs postes de travail	Permet d'autoriser les utilisateurs à réinitialiser leurs propres postes de travail sans assistance administrative.
Autoriser plusieurs sessions par utilisateur	Permet d'autoriser un utilisateur à se connecter simultanément à plusieurs postes de travail du pool.
Supprimer le poste de travail après la fermeture de session	Indiquez si vous souhaitez supprimer les postes de travail de machines virtuelles complètes d'affectation flottante. ■ **[Non]** . Les machines virtuelles restent dans le pool de postes de travail quand les utilisateurs ferment leur session. ■ **[Oui]** . Les machines virtuelles sont désactivées et supprimées dès que les utilisateurs ferment leur session.
Supprimer ou actualiser le poste de travail à la fermeture de session	Choisissez de supprimer, d'actualiser ou de ne pas modifier des postes de travail de clone lié d'affectation flottante. ■ **[Jamais]** . Les machines virtuelles restent dans le pool et ne sont pas actualisées quand les utilisateurs ferment leur session. ■ **[Supprimer immédiatement]** . Les machines virtuelles sont désactivées et supprimées dès que les utilisateurs ferment leur session. Lorsque des utilisateurs ferment leur session, View Manager met immédiatement les machines virtuelles en état `Suppression`. ■ **[Actualiser immédiatement]** . Les machines virtuelles sont actualisées dès que les utilisateurs ferment leur session. Lorsque des utilisateurs ferment leur session, View Manager met immédiatement les machines virtuelles en mode de maintenance pour empêcher d'autres utilisateurs d'ouvrir une session lorsque l'opération d'actualisation démarre.

Tableau 5-19. Descriptions des paramètres de poste de travail et de pool (suite)

Paramètre	Options
Actualiser le disque du système d'exploitation après la fermeture de session	Choisissez d'actualiser, et quand actualiser, les disques du système d'exploitation pour des postes de travail de clone lié d'affectation dédiée. ■ **[Jamais]** . Le disque du système d'exploitation n'est jamais actualisé. ■ **[Toujours]** . Le disque du système d'exploitation est actualisé chaque fois que l'utilisateur ferme sa session. ■ **[Tous les]** . Le disque du système d'exploitation est actualisé à intervalles réguliers sur un nombre spécifié de jours. Saisissez le nombre de jours. Le nombre de jours est compté depuis la dernière actualisation, ou depuis l'approvisionnement initial si aucune actualisation ne s'est encore produite. Par exemple, si la valeur spécifiée est **3** jours, et si trois jours ont passé depuis la dernière actualisation, le poste de travail est actualisé lorsque l'utilisateur ferme sa session. ■ **[À]** . Le disque du système d'exploitation est actualisé lorsque sa taille actuelle atteint le pourcentage spécifié de sa taille maximale autorisée. La taille maximale du disque du système d'exploitation d'un clone lié est la taille du disque du système d'exploitation du réplica. Saisissez le pourcentage auquel les opérations d'actualisation se produisent. Avec l'option **[À]** , la taille du disque du système d'exploitation du clone lié dans le magasin de données est comparée à sa taille maximale autorisée. Ce pourcentage d'utilisation du disque ne reflète pas l'utilisation du disque que vous pouvez voir dans le système d'exploitation client du poste de travail. Lorsque vous actualisez les disques du système d'exploitation dans un pool de clone lié avec affectation dédiée, les disques persistants de View Composer ne sont pas affectés.
Protocole d'affichage par défaut	Sélectionnez le protocole d'affichage que vous voulez que Serveur de connexion View utilise pour communiquer avec des clients View. **PCoIP** — Option par défaut quand prise en charge. PCoIP est pris en charge en tant que protocole d'affichage pour les postes de travail de machine virtuelle et les machines physiques ayant un matériel Teradici. PCoIP offre une utilisation optimisée du PC pour délivrer des images, du contenu audio et vidéo à un grand nombre d'utilisateurs sur le réseau LAN ou sur le réseau WAN. **Microsoft RDP** — La Connexion Bureau à distance Microsoft utilise RDP pour transmettre des données. RDP est un protocole multicanal qui permet à un utilisateur de se connecter à distance à un ordinateur.
Autoriser les utilisateurs à choisir un protocole	Permet d'autoriser les utilisateurs à remplacer le protocole d'affichage par défaut pour leurs postes de travail en utilisant View Client.

Tableau 5-19. Descriptions des paramètres de poste de travail et de pool (suite)

Paramètre	Options
Convertisseur 3D	Vous pouvez choisir d'activer le rendu graphique 3D si votre pool comporte des postes de travail Windows 7 ou supérieur. Vous pouvez configurer **[Convertisseur 3D]** afin qu'il utilise le rendu logiciel ou le rendu matériel en fonction des cartes de processeur graphique physiques installées sur les hôtes ESXi 5.1 ou supérieur. Pour activer cette fonction, vous devez sélectionner PCoIP comme protocole et désactiver le paramètre **[Autoriser les utilisateurs à choisir un protocole]** (sélectionnez **[Non]**). Avec les options de **[Convertisseur 3D]** basé sur le matériel, les utilisateurs peuvent bénéficier des applications graphiques pour la conception, la modélisation et le multimédia. Les postes de travail doivent être exécutés sur vSphere 5.1 ou supérieur. Les postes de travail Windows 7 doivent avoir la version matérielle virtuelle 8 ou supérieure. Les postes de travail Windows 8 doivent avoir la version matérielle virtuelle 9 ou supérieure. Avec l'option de **[Convertisseur 3D]** logiciel, les utilisateurs peuvent bénéficier d'améliorations graphiques des applications moins gourmandes, telles qu'AERO, Microsoft Office 2010 et Google Earth. Les postes de travail doivent être exécutés sur vSphere 5.0 ou supérieur et avoir la version matérielle virtuelle 8 ou supérieure. Si votre déploiement de View n'est pas exécuté sur vSphere 5.0 ou supérieur, ce paramètre n'est pas disponible et est inactif dans View Administrator. Lorsque vous sélectionnez cette fonction, vous pouvez configurer la quantité de VRAM affectée à des postes de travail dans le pool. Vous pouvez sélectionner au plus deux écrans pour vos postes de travail View. La valeur **[Résolution max. d'un écran]** est définie sur 1920x1200 pixels. Vous ne pouvez pas configurer cette valeur. **Remarque** Vous devez désactiver et activer des machines virtuelles existantes pour que ce paramètre prenne effet. Le redémarrage d'une machine virtuelle n'entraîne pas la prise d'effet du paramètre. Pour plus d'informations, reportez-vous aux sections « Configuration du rendu 3D sur des postes de travail Windows 7 ou supérieur », page 156, « Options de rendu 3D », page 158 et « Meilleures pratiques pour la configuration du rendu 3D », page 159.
Nombre max. d'écrans	Si vous utilisez PCoIP comme protocole d'affichage, vous pouvez sélectionner le **[Nombre max. d'écrans]** sur lesquels les utilisateurs peuvent afficher le poste de travail. Lorsque le paramètre **[Convertisseur 3D]** n'est pas sélectionné, le paramètre Nombre max. d'écrans affecte la quantité de VRAM affectée à des postes de travail dans le pool. Lorsque vous augmentez le nombre d'écrans, davantage de mémoire est consommée sur les hôtes ESXi associés. Lorsque le paramètre **[Convertisseur 3D]** est sélectionné, vous pouvez sélectionner au plus deux écrans. **Remarque** Vous devez désactiver et activer des machines virtuelles existantes pour que ce paramètre prenne effet. Le redémarrage d'une machine virtuelle n'entraîne pas la prise d'effet du paramètre.

Tableau 5-19. Descriptions des paramètres de poste de travail et de pool (suite)

Paramètre	Options
Résolution max. d'un écran	Si vous utilisez PCoIP comme protocole d'affichage et si vous ne sélectionnez pas le paramètre **[Convertisseur 3D]** , vous devez spécifier la **[Résolution max. d'un écran]** . Lorsque le paramètre **[Convertisseur 3D]** n'est pas sélectionné, le paramètre Résolution max. d'un écran affecte la quantité de VRAM affectée à des postes de travail dans le pool. Lorsque vous augmentez la résolution, davantage de mémoire est consommée sur les hôtes ESX associés. Lorsque le paramètre **[Convertisseur 3D]** est sélectionné, vous ne pouvez pas modifier la **[Résolution max. d'un écran]** . La résolution est définie sur 1920 x 1200 pixels. **Remarque** Vous devez désactiver et activer des machines virtuelles existantes pour que ce paramètre prenne effet. Le redémarrage d'une machine virtuelle n'entraîne pas la prise d'effet du paramètre.
HTML Access	Détermine si les utilisateurs sont autorisés à se connecter à des postes de travail View via HTML depuis leurs navigateurs Web. Sélectionnez **[Activé]** pour autoriser des utilisateurs Horizon à se connecter à des postes de travail View dans ce pool via HTML. Lorsqu'un utilisateur se connecte à View Portal ou Horizon User Portal et qu'il sélectionne un poste de travail View, Blast Agent permet à l'utilisateur de se connecter au poste de travail via HTTPS. Le poste de travail est affiché dans le navigateur de l'utilisateur. D'autres protocoles d'affichage, tels que PCoIP ou RDP, ne sont pas utilisés. Le logiciel View Client n'a pas à être installé sur les périphériques client. Pour utiliser l'accès HTML, vous devez installer le pack de fonctionnalités d'accès HTML au poste de travail dans votre déploiement de View. Blast Agent doit être installé sur les postes de travail View dans le pool. Pour utiliser HTML Access avec Horizon Workspace, vous devez coupler Serveur de connexion View avec un serveur d'authentification SAML 2.0. Horizon Workspace doit être installé et configuré pour être utilisé avec Serveur de connexion View.

Tableau 5-19. Descriptions des paramètres de poste de travail et de pool (suite)

Paramètre	Options
Qualité Adobe Flash	Détermine la qualité du contenu Adobe Flash affiché sur des pages Web. ■ **[Ne pas contrôler]** . La qualité est déterminée par les paramètres de page Web. ■ **[Faible]** . Ce paramètre se traduit par les meilleures économies de bande passante. Si aucun niveau de qualité n'est spécifié, le système prend la valeur par défaut Faible. ■ **[Moyenne]** . Ce paramètre se traduit par des économies de bande passante modérées. ■ **[Haute]** . Ce paramètre se traduit par des économies de bande passante moindres. Pour plus d'informations, reportez-vous à la section « Qualité et limitation d'Adobe Flash », page 312.
Limitation d'Adobe Flash	Détermine la fréquence d'image des films Adobe Flash. Si vous activez ce paramètre, vous pouvez réduire ou augmenter le nombre d'images affichées par seconde en sélectionnant un niveau d'agressivité. ■ **[Désactivé]** . Aucune limitation n'est effectuée. L'intervalle du temporisateur n'est pas modifié. ■ **[Conservateur]** . L'intervalle du temporisateur est de 100 millisecondes. Ce paramètre correspond au plus petit nombre d'images ignorées. ■ **[Modéré]** . L'intervalle du temporisateur est de 500 millisecondes. ■ **[Agressif]** . L'intervalle du temporisateur est de 2 500 millisecondes. Ce paramètre correspond au plus grand nombre d'images ignorées. Pour plus d'informations, reportez-vous à la section « Qualité et limitation d'Adobe Flash », page 312.

Remarque Les propriétés définies pour les postes de travail locaux n'ont aucun effet tant que les postes de travail ne sont pas restitués.

Configuration du rendu 3D sur des postes de travail Windows 7 ou supérieur

Lorsque vous créez ou modifiez un pool de postes de travail Windows 7 ou supérieur, vous pouvez configurer un rendu graphique 3D pour vos postes de travail. Les postes de travail peuvent bénéficier de vSGA (Virtual Shared Graphics Acceleration), une fonction de vSphere qui utilise des cartes graphiques physiques installées sur les hôtes ESXi et qui gère les ressources de processeur graphique parmi les postes de travail.

Lorsque vous sélectionnez les options basées sur le matériel **[Convertisseur 3D]** , les utilisateurs peuvent bénéficier d'applications 3D pour la conception, la modélisation et le multimédia, qui exigent généralement du matériel de processeur graphique pour être exécutées correctement. Le paramètre **[Convertisseur 3D]** offre également une option logicielle, qui fournit des améliorations graphiques pouvant prendre en charge des applications moins gourmandes, telles que Windows AERO, Microsoft Office 2010 et Google Earth.

Exigences pour le rendu 3D

Pour activer le rendu graphique 3D matériel ou logiciel, votre déploiement de pools doit répondre aux exigences suivantes :

- Les postes de travail doivent être Windows 7 ou supérieur
- Le pool doit utiliser PCoIP comme protocole d'affichage par défaut
- Les utilisateurs ne doivent pas être autorisés à choisir leur propre protocole

Pour prendre en charge le rendu 3D basé sur le matériel, un pool doit répondre aux exigences supplémentaires suivantes :

- Les postes de travail doivent s'exécuter sur des hôtes ESXi 5.1 ou supérieur et être gérés par le logiciel vCenter Server 5.1 ou supérieur
- Les cartes de processeur graphique et les VIB (vSphere Installation Bundle) associés doivent être installés sur les hôtes ESXi. Pour voir une liste du matériel de processeur graphique pris en charge, consultez la liste de compatibilité matérielle VMware à l'adresse http://www.vmware.com/resources/compatibility/search.php.
- Les postes de travail Windows 7 doivent avoir la version matérielle virtuelle 8 ou supérieure. Les postes de travail Windows 8 doivent avoir la version matérielle virtuelle 9 ou supérieure.

Pour prendre en charge le rendu 3D logiciel, un pool doit répondre aux exigences supplémentaires suivantes :

- Les postes de travail doivent s'exécuter sur des hôtes ESXi 5.0 ou supérieur et être gérés par le logiciel vCenter Server 5.0 ou supérieur
- Les postes de travail doivent avoir la version matérielle virtuelle 8 ou supérieure

Vous devez désactiver et activer des machines virtuelles existantes pour que le paramètre **[Convertisseur 3D]** prenne effet. Le redémarrage d'une machine virtuelle n'entraîne pas la prise d'effet du paramètre.

Configuration du rendu 3D

Vous sélectionnez des options pour déterminer la façon dont View gère le rendu 3D. Pour plus d'informations, reportez-vous à la section « Options de rendu 3D », page 158.

Lorsque vous activez le paramètre **[Convertisseur 3D]**, vous pouvez configurer la quantité de VRAM affectée aux postes de travail dans le pool en déplaçant le curseur dans la boîte de dialogue Configurer VRAM pour des clients 3D. La taille VRAM minimale est de 64 Mo. Pour les machines virtuelles avec la version matérielle virtuelle 9, la taille VRAM par défaut est de 96 Mo et vous pouvez configurer une taille maximale de 512 Mo. Pour les machines virtuelles avec la version matérielle virtuelle 8, la taille VRAM par défaut est de 64 Mo et vous pouvez configurer une taille maximale de 128 Mo.

Les paramètres VRAM que vous configurez dans View Administrator sont prioritaires sur les paramètres VRAM qui peuvent être configurés pour les machines virtuelles dans vSphere Client ou vSphere Web Client, sauf si vous sélectionnez l'option **[Gérer à l'aide de vSphere Client]**.

Lorsque vous activez le paramètre **[Convertisseur 3D]**, vous pouvez configurer le paramètre **[Nombre max. d'écrans]** pour un ou deux écrans. Vous ne pouvez pas sélectionner plus de deux écrans. De plus, le paramètre **[Résolution max. d'un écran]** est défini sur 1920 x 1200 pixels.

Options de rendu 3D

Le paramètre **[Convertisseur 3D]** pour les pools de postes de travail fournit des options vous permettant de configurer le rendu graphique de différentes façons.

Tableau 5-20. Options du convertisseur 3D pour les pools exécutés sur vSphere 5.1 ou supérieur

Option	Description
Gérer à l'aide de vSphere Client	L'option **[Convertisseur 3D]** définie dans vSphere Web Client pour une machine virtuelle détermine le type de rendu graphique 3D qui a lieu. View ne contrôle pas le rendu 3D. Dans vSphere Web Client, vous pouvez configurer les options **[Automatique]**, **[Logiciel]** ou **[Matériel]**. Ces options ont le même effet que lorsque vous les définissez dans View Administrator. Lorsque vous sélectionnez l'option **[Gérer à l'aide de vSphere Client]**, les paramètres **[Configurer VRAM pour des clients 3D]**, **[Nombre max. d'écrans]** et **[Résolution max. d'un écran]** sont inactifs dans View Administrator. Vous pouvez configurer ces paramètres pour une machine virtuelle dans vSphere Web Client.
Automatique	Le rendu 3D est activé. L'hôte ESXi contrôle le type de rendu 3D qui a lieu. Par exemple, l'hôte ESXi réserve des ressources matérielles de processeur graphique sur la base « premier arrivé, premier servi » à mesure que les machines virtuelles sont activées. Si toutes les ressources matérielles de processeur graphique sont déjà réservées lorsqu'une machine virtuelle est activée, ESXi utilise le convertisseur logiciel pour cette machine. Lorsque vous configurez le rendu 3D basé sur le matériel, vous pouvez examiner les ressources de processeur graphique qui sont allouées à chaque machine virtuelle sur un hôte ESXi. Pour plus d'informations, reportez-vous à la section « Examen des ressources de processeur graphique sur un hôte ESXi », page 160.
Logiciel	Le rendu 3D est activé. L'hôte ESXi utilise le rendu graphique 3D logiciel. Si une carte de processeur graphique est installée sur l'hôte ESXi, ce pool ne l'utilisera pas. Dans la boîte de dialogue Configurer VRAM pour des clients 3D, vous pouvez utiliser le curseur pour augmenter la quantité de VRAM réservée.
Matériel	Le rendu 3D est activé. L'hôte ESXi réserve des ressources matérielles de processeur graphique sur la base « premier arrivé, premier servi » à mesure que les machines virtuelles sont activées. L'hôte ESXi alloue de la VRAM à une machine virtuelle en fonction de la valeur définie dans la boîte de dialogue Configurer VRAM pour des clients 3D. IMPORTANT Si vous configurez l'option **[Matériel]**, tenez compte des contraintes potentielles suivantes : ■ Si un utilisateur tente de se connecter à un poste de travail lorsque toutes les ressources matérielles de processeur graphique sont réservées, la machine virtuelle ne s'active pas et l'utilisateur reçoit un message d'erreur. ■ Un poste de travail ne peut pas être déplacé par vMotion vers un hôte ESXi sur lequel le matériel de processeur graphique n'est pas configuré. ■ La version de tous les hôtes ESXi dans le cluster doit être la version 5.1 ou supérieure. Si un poste de travail est créé sur un hôte ESXi 5.0 dans un cluster mélangé, la machine virtuelle ne s'active pas. Lorsque vous configurez le rendu 3D basé sur le matériel, vous pouvez examiner les ressources de processeur graphique qui sont allouées à chaque machine virtuelle sur un hôte ESXi. Pour plus d'informations, reportez-vous à la section « Examen des ressources de processeur graphique sur un hôte ESXi », page 160.
Désactivée	Le rendu 3D est inactif.

Tableau 5-21. Options du convertisseur 3D pour les pools exécutés sur vSphere 5.0

Option	Description
Activée	L'option **[Convertisseur 3D]** est activée. L'hôte ESXi utilise le rendu graphique 3D logiciel. Lorsque le rendu logiciel est configuré, la taille VRAM par défaut est de 64 Mo, la taille minimale. Dans la boîte de dialogue Configurer VRAM pour des clients 3D, vous pouvez utiliser le curseur pour augmenter la quantité de VRAM réservée. Avec le rendu logiciel, l'hôte ESXi alloue jusqu'à 128 Mo maximum par machine virtuelle. Si vous définissez une taille VRAM supérieure, elle est ignorée.
Désactivée	Le rendu 3D est inactif.

Si un pool de postes de travail est exécuté sur une version de vSphere antérieure à 5.0, le paramètre **[Convertisseur 3D]** est inactif et n'est pas disponible dans View Administrator.

Meilleures pratiques pour la configuration du rendu 3D

Les options de rendu 3D et d'autres paramètres de pool présentent divers avantages et inconvénients. Sélectionnez l'option la plus adaptée à votre infrastructure matérielle vSphere et aux exigences de vos utilisateurs pour le rendu graphique.

L'option **[Automatique]** est le meilleur choix pour les déploiements de View qui exigent le rendu 3D. Cette option garantit qu'un certain type de rendu 3D a lieu même lorsque des ressources de processeur graphique sont entièrement réservées. Dans un cluster mélangé d'hôtes ESXi 5.1 et ESXi 5.0, cette option garantit qu'une machine virtuelle est activée correctement et qu'elle utilise le rendu 3D même si, par exemple, vMotion a déplacé la machine virtuelle vers un hôte ESXi 5.0.

Le seul inconvénient de l'option **[Automatique]** est que vous ne pouvez pas facilement voir si une machine virtuelle utilise le rendu 3D matériel ou logiciel.

L'option **[Matériel]** garantit que chaque machine virtuelle dans le pool utilise le rendu 3D matériel, à condition que des ressources de processeur graphique soient disponibles sur les hôtes ESXi. Cette option peut représenter le meilleur choix lorsque tous les utilisateurs exécutent des applications gourmandes en ressources graphiques.

Avec l'option **[Matériel]** , vous devez contrôler votre environnement vSphere de façon stricte. La version de tous les hôtes ESXi doit être la version 5.1 ou supérieure et des cartes de processeur graphique doivent être installées sur ces hôtes. Lorsque toutes les ressources de processeur graphique sur un hôte ESXi sont réservées, View ne peut pas activer une machine virtuelle pour l'utilisateur suivant qui tente de se connecter à un poste de travail. Vous devez gérer l'allocation de ressources de processeur graphique et l'utilisation de vMotion afin de garantir que des ressources sont disponibles pour vos postes de travail.

Sélectionnez l'option **[Gérer à l'aide de vSphere Client]** pour prendre en charge une configuration mélangée de rendu 3D et de tailles de VRAM pour les machines virtuelles dans un pool. Dans vSphere Web Client, vous pouvez configurer des machines virtuelles individuelles avec différentes options et valeurs VRAM.

Sélectionnez l'option **[Logiciel]** si vous ne disposez que d'hôtes ESXi 5.0, si les hôtes ESXi 5.1 ne contiennent pas de cartes de processeur graphique ou si vos utilisateurs exécutent uniquement des applications, telles qu'AERO et Microsoft Office, qui n'exigent pas l'accélération graphique matérielle.

Configuration de paramètres de poste de travail pour gérer des ressources de processeur graphique

Vous pouvez configurer d'autres paramètres de poste de travail pour garantir que les ressources de processeur graphique ne sont pas gaspillées lorsque les utilisateurs ne les utilisent pas activement.

Pour les pools flottants, définissez un délai d'expiration de session pour que les ressources de processeur graphique soient libérées pour les autres utilisateurs lorsqu'un utilisateur n'utilise pas le poste de travail.

Pour les pools dédiés, vous pouvez configurer le paramètre **[Fermeture de session automatique après la déconnexion]** sur **[Immédiatement]** et une règle d'alimentation **[Interrompre]** si ces paramètres sont appropriés pour vos utilisateurs. Par exemple, n'utilisez pas ces paramètres pour un groupe de chercheurs qui exécutent de longues simulations.

Examen des ressources de processeur graphique sur un hôte ESXi

Pour mieux gérer les ressources de processeur graphique disponibles sur un hôte ESXi, vous pouvez examiner la réservation de ressources de processeur graphique actuelle. L'utilitaire de requête de ligne de commande ESXi, `gpuvm`, répertorie les processeurs graphiques installés sur un hôte ESXi et affiche la quantité de mémoire de processeur graphique réservée pour chaque machine virtuelle sur l'hôte. Notez que cette réservation de mémoire de processeur graphique n'est pas la même que la taille VRAM de machine virtuelle.

Pour exécuter l'utilitaire, tapez **`gpuvm`** dans une invite du shell sur l'hôte ESXi. Vous pouvez utiliser une console sur l'hôte ou une connexion SSH.

Par exemple, l'utilitaire peut afficher la sortie suivante :

```
~ # gpuvm
Xserver unix:0, GPU maximum memory 2076672KB
        pid 118561, VM "JB-w7-64-FC3", reserved 131072KB of GPU memory.
        pid 64408, VM "JB-w7-64-FC5", reserved 261120KB of GPU memory.
        GPU memory left 1684480KB.
```

Empêcher l'accès à des postes de travail View via RDP

Dans certains environnements View, interdire l'accès à des postes de travail View via le protocole d'affichage RDP est une priorité. Vous pouvez empêcher des utilisateurs et des administrateurs d'utiliser RDP pour accéder à des postes de travail View en configurant des paramètres de pool et un paramètre de stratégie de groupe.

Par défaut, lorsqu'un utilisateur a ouvert une session sur un poste de travail View, vous pouvez utiliser RDP pour vous connecter à la machine virtuelle de poste de travail depuis l'extérieur de View. La connexion RDP met fin à la session du poste de travail View et les données et paramètres non enregistrés de l'utilisateur View peuvent être perdus. L'utilisateur View ne peut pas ouvrir de session sur le poste de travail tant que la connexion RDP externe n'est pas fermée. Pour éviter cette situation, désactivez le paramètre `AllowDirectRDP`.

Remarque Les services Bureau à distance, appelés Terminal Services sur les systèmes Windows XP, doivent être démarrés sur la machine virtuelle que vous utilisez pour créer des pools et sur des postes de travail View. Les services Bureau à distance sont requis pour l'installation de View Agent, l'authentification unique et d'autres opérations de gestion des sessions de View.

Prérequis

Vérifiez que le fichier de modèle d'administration de configuration de View Agent est installé dans Active Directory. Reportez-vous à la section « Utilisation de fichiers de modèle d'administration de stratégie de groupe de View », page 207.

Procédure

1 Sélectionnez PCoIP comme protocole d'affichage que vous voulez que Serveur de connexion View utilise pour communiquer avec des clients View.

Option	Description
Créer un pool de postes de travail	a Dans View Administrator, démarrez l'assistant Ajouter un pool. b Sur la page Paramètres de poste de travail, sélectionnez **[PCoIP]** comme protocole d'affichage par défaut.
Modifier un pool de postes de travail existant	a Dans View Administrator, sélectionnez le pool de postes de travail et cliquez sur **[Modifier]** . b Sélectionnez l'onglet Paramètres de pool et sélectionnez **[PCoIP]** comme protocole d'affichage par défaut.

2 Pour le paramètre **[Autoriser les utilisateurs à choisir un protocole]** , sélectionnez **[Non]** .

3 Empêchez les clients non View de se connecter directement à des postes de travail View via RDP en désactivant le paramètre de stratégie de groupe `AllowDirectRDP`.

   a Sur votre serveur Active Directory, ouvrez la Console de gestion des stratégies de groupe et sélectionnez **[Configuration ordinateur] > [Modèles administratifs] > [Configuration de VMware View Agent]** .

   b Désactivez le paramètre `AllowDirectRDP`.

Définition de règles d'alimentation pour des pools de postes de travail

Vous pouvez configurer une règle d'alimentation pour les machines virtuelles d'un pool de postes de travail si les machines virtuelles sont gérées par vCenter Server.

Les règles d'alimentation contrôlent comment une machine virtuelle se comporte lorsque son poste de travail associé n'est pas utilisé. Un poste de travail est considéré comme n'étant pas utilisé avant qu'un utilisateur ouvre une session et après qu'un utilisateur se déconnecte ou ferme sa session. Les règles d'alimentation contrôlent également comment une machine virtuelle se comporte après l'exécution de tâches administratives, telles qu'une actualisation, une recomposition et un rééquilibrage.

Vous configurez des règles d'alimentation lorsque vous créez ou modifiez des pools de postes de travail dans View Administrator. Reportez-vous à la section Chapitre 5, « Création de pools de postes de travail », page 97 ou « Gestion de pools de postes de travail », page 305 pour plus d'informations.

Remarque Vous ne pouvez pas configurer de règles d'alimentation pour des pools de postes de travail qui possèdent des postes de travail non gérés.

Règles d'alimentation pour des pools de postes de travail

Les règles d'alimentation contrôlent comment une machine virtuelle se comporte lorsque le poste de travail View associé n'est pas utilisé.

Vous définissez des règles d'alimentation lorsque vous créez ou modifiez un pool de postes de travail. Tableau 5-22 décrit les règles d'alimentation disponibles.

Tableau 5-22. Règles d'alimentation

Règle d'alimentation	Description
[Ne prendre aucune action d'alimentation]	View Manager n'applique aucune règle d'alimentation quand un utilisateur ferme sa session. Ce paramètre a deux conséquences. ■ View Manager ne modifie pas l'état d'alimentation de la machine virtuelle quand un utilisateur ferme sa session. Par exemple, si un utilisateur éteint la machine virtuelle, celle-ci reste désactivée. Si un utilisateur ferme sa session sans éteindre, la machine virtuelle reste activée. Lorsqu'un utilisateur se reconnecte au poste de travail, la machine virtuelle redémarre si elle a été désactivée. ■ View Manager n'applique aucun état d'alimentation quand une tâche administrative est effectuée. Par exemple, un utilisateur peut fermer sa session sans éteindre. La machine virtuelle reste activée. Quand une recomposition planifiée a lieu, la machine virtuelle est désactivée. Après la recomposition, View Manager ne fait rien pour modifier l'état d'alimentation de la machine virtuelle. Elle reste désactivée.
[S'assurer que les postes de travail sont toujours activés]	La machine virtuelle reste activée, même lorsqu'elle n'est pas utilisée. Si un utilisateur éteint la machine virtuelle, elle redémarre immédiatement. La machine virtuelle redémarre également après l'exécution d'une tâche administrative, telle qu'une actualisation, une recomposition ou un rééquilibrage. Sélectionnez **[S'assurer que les postes de travail sont toujours activés]** si vous exécutez des processus de traitement par lot ou des outils de gestion de système qui doivent contacter les machines virtuelles à des heures planifiées.
[Interrompre]	La machine virtuelle est interrompue quand un utilisateur ferme sa session, mais pas quand il se déconnecte. Vous pouvez également configurer des postes de travail dans un pool dédié pour qu'il soit interrompu lorsqu'un utilisateur se déconnecte sans fermer sa session. Pour configurer cette règle, vous devez définir un attribut dans View LDAP. Reportez-vous à la section « Configurer des postes de travail dédiés pour les suspendre après la déconnexion des utilisateurs », page 164. Lorsque plusieurs machines virtuelles reprennent après avoir été interrompues, l'activation de certaines d'entre elles peut être retardée. Les retards dépendent du matériel de l'hôte ESXi et du nombre de machines virtuelles configurées sur un hôte ESXi. Les utilisateurs se connectant à leurs postes de travail depuis View Client peuvent voir temporairement un message indiquant que le poste de travail n'est pas disponible. Pour accéder à leurs postes de travail, les utilisateurs peuvent se reconnecter.
[Désactiver]	La machine virtuelle s'éteint quand un utilisateur ferme sa session, mais pas quand il se déconnecte.

Remarque Lorsque vous ajoutez un poste de travail à un pool manuel, View Manager active le poste de travail pour s'assurer qu'il est complètement configuré, même lorsque vous sélectionnez la règle d'alimentation **[Désactiver]** ou **[Ne prendre aucune action d'alimentation]** . Quand View Agent est configuré, il est marqué comme étant Prêt et les paramètres normaux de gestion d'alimentation pour le pool s'appliquent.

Pour les pools manuels avec des postes de travail gérés par vCenter Server, View Manager garantit qu'un poste de travail de rechange est activé afin que les utilisateurs puissent s'y connecter. Le poste de travail de rechange est activé quelle que soit la règle d'alimentation appliquée.

Tableau 5-23 décrit quand View Manager applique la règle d'alimentation configurée.

Tableau 5-23. Quand View Manager applique la règle d'alimentation

Type de pool de postes de travail	La règle d'alimentation est appliquée...
Pool manuel contenant un poste de travail (machine virtuelle gérée par vCenter Server)	Les opérations d'alimentation sont initiées par la gestion des sessions. La machine virtuelle est activée lorsqu'un utilisateur demande le poste de travail, et désactivée ou interrompue quand l'utilisateur ferme sa session. **Remarque** La règle **[S'assurer que les postes de travail sont toujours activés]** s'applique toujours, que le pool de poste de travail unique utilise une affectation flottante ou dédiée, et que le poste de travail soit affecté ou pas.
Pool automatisé avec affectation dédiée	Uniquement à des postes de travail non affectés. Sur les postes de travail affectés, les opérations d'alimentation sont initiées par la gestion des sessions. Les machines virtuelles sont activées lorsqu'un utilisateur demande un poste de travail affecté et désactivées ou interrompues quand l'utilisateur ferme sa session. **Remarque** La règle **[S'assurer que les postes de travail sont toujours activés]** s'applique aux postes de travail affectés et non affectés.
Pool automatisé avec affectation flottante	Quand un poste de travail n'est pas utilisé et après la fermeture de session d'un utilisateur. Lorsque vous configurez la règle d'alimentation **[Désactiver]** ou **[Interrompre]** pour un pool de postes de travail d'affectation flottante, définissez **[Fermeture de session automatique après la déconnexion]** sur **[Immédiatement]** pour empêcher les sessions ignorées ou orphelines.
Pool manuel avec affectation dédiée	Uniquement à des postes de travail non affectés. Sur les postes de travail affectés, les opérations d'alimentation sont initiées par la gestion des sessions. Les machines virtuelles sont activées lorsqu'un utilisateur demande un poste de travail affecté et désactivées ou interrompues quand l'utilisateur ferme sa session. **Remarque** La règle **[S'assurer que les postes de travail sont toujours activés]** s'applique aux postes de travail affectés et non affectés.
Pool manuel avec affectation flottante	Quand un poste de travail n'est pas utilisé et après la fermeture de session d'un utilisateur. Lorsque vous configurez la règle d'alimentation **[Désactiver]** ou **[Interrompre]** pour un pool de postes de travail d'affectation flottante, définissez **[Fermeture de session automatique après la déconnexion]** sur **[Immédiatement]** pour empêcher les sessions ignorées ou orphelines.

La façon dont View Manager applique la règle d'alimentation configurée à des pools automatisés dépend de la disponibilité d'un poste de travail. Reportez-vous à la section « Comment les règles d'alimentation affectent les pools automatisés », page 164 pour plus d'informations.

Configurer des postes de travail dédiés pour les suspendre après la déconnexion des utilisateurs

La stratégie d'alimentation **[Suspend (Suspendre)]** suspend les machines virtuelles lorsque l'utilisateur ferme une session, mais pas lorsqu'il se déconnecte. Vous pouvez également configurer les postes de travail dans un pool dédié à suspendre lorsqu'un utilisateur se déconnecte d'un poste de travail sans fermer de session. La suspension des utilisateurs lorsqu'ils se déconnectent permet d'économiser les ressources.

Pour activer la suspension à la déconnexion pour des postes de bureau dédiés, vous devez définir un attribut dans View LDAP.

Procédure

1 Démarrez l'utilitaire ADSI Edit sur votre hôte de Serveur de connexion View.

2 Dans l'arborescence de console, sélectionnez **[Connect to (Se connecter à)]** .

3 Dans le champ **[Select or type a domain or server (Sélectionner ou taper un domaine ou un serveur)]** , tapez le nom de serveur **`localhost:389`**

4 Sous **[Connection point (Point de connexion)]** , cliquez sur **[Select or type a distinguished name or naming context (Sélectionner ou taper un nom unique ou un contexte de dénomination)]** , tapez le nom unique **`DC=vdi,DC=vmware,DC=int`**, puis cliquez sur **[OK]** .

   La fenêtre principale ADAM ADSI Edit (Édition ADAM ADSI) s'affiche.

5 Développez l'arborescence ADAM ADSI et **[OU=Properties]** .

6 Sélectionnez **[OU=Global]** et **[CN=Common]** dans le volet de droite.

7 Sélectionnez **[Action] > [Properties (propriétés)]** , puis sous l'attribut **[pae-NameValuePair]** , ajoutez l'entrée **`suspendOnDisconnect=1`**.

8 Redémarrez Serveur de connexion View.

Comment les règles d'alimentation affectent les pools automatisés

La façon dont View applique la règle d'alimentation configurée à des pools automatisés dépend de la disponibilité d'un poste de travail View.

Un poste de travail dans un pool automatisé est considéré comme étant disponible lorsqu'il satisfait les critères suivants :

- Il est actif.
- Il ne contient pas de session utilisateur.
- Il n'est pas affecté à un utilisateur.

Le service View Agent exécuté sur le poste de travail confirme la disponibilité du poste de travail à View Connection Server.

Lorsque vous configurez un pool automatisé, vous pouvez spécifier le nombre minimum et maximum de machines virtuelles devant être approvisionnées et le nombre de postes de travail de rechange devant rester alimentés et devant être disponibles à n'importe quel moment donné.

Exemples de règle d'alimentation pour des pools automatisés avec des affectations flottantes

Lorsque vous configurez un pool automatisé avec des affectations flottantes, vous pouvez spécifier qu'un nombre particulier de postes de travail View doit être disponible à une heure donnée. Les postes de travail de rechange disponibles sont toujours activés, quelle que soit la définition de la règle de pool.

Exemple 1 de règle d'alimentation

Tableau 5-24 décrit le pool automatisé d'affectation flottante dans cet exemple. Le pool utilise un mode d'attribution de nom pour approvisionner et nommer les postes de travail.

Tableau 5-24. Exemple 1 des paramètres de pool de postes de travail d'un pool automatisé avec une affectation flottante

Paramètre du pool de postes de travail	Valeur
Nombre de postes de travail (minimum)	10
Nombre de postes de travail (maximum)	20
Nombre de postes de travail de rechange activés	2
Règle d'alimentation de poste de travail distant	Désactiver

Lorsque ce pool de postes de travail est approvisionné, 10 postes de travail sont créés, 2 postes de travail sont activés et immédiatement disponibles et 8 postes de travail sont désactivés.

Pour chaque nouvel utilisateur qui se connecte au pool, un poste de travail est activé pour conserver le nombre de postes de travail de rechange disponibles. Lorsque le nombre d'utilisateurs connectés dépasse 8, des postes de travail supplémentaires (20 maximum) sont créés pour conserver le nombre de postes de travail de rechange. Quand le nombre maximum est atteint, les postes de travail des deux premiers utilisateurs qui se déconnectent restent activés pour conserver le nombre de postes de travail de rechange. Le poste de travail de chaque utilisateur suivant est désactivé en fonction de la règle d'alimentation.

Exemple 2 de règle d'alimentation

Tableau 5-25 décrit le pool automatisé d'affectation flottante dans cet exemple. Le pool utilise un mode d'attribution de nom pour approvisionner et nommer les postes de travail.

Tableau 5-25. Exemple 2 des paramètres de pool de postes de travail d'un pool automatisé avec des affectations flottantes

Paramètre du pool de postes de travail	Valeur
Nombre de postes de travail (minimum)	5
Nombre de postes de travail (maximum)	5
Nombre de postes de travail de rechange activés	2
Règle d'alimentation de poste de travail distant	Désactiver

Lorsque ce pool de postes de travail est approvisionné, 5 postes de travail sont créés, 2 postes de travail sont activés et immédiatement disponibles et 3 postes de travail sont désactivés.

Si un quatrième poste de travail dans ce pool est désactivé, l'un des postes de travail existants est activé. Aucun poste de travail supplémentaire n'est activé car le nombre maximum de postes de travail a déjà été atteint.

Exemple de règle d'alimentation pour des pools automatisés avec des affectations dédiées

Contrairement à un poste de travail View activé dans un pool automatisé avec des affectations flottantes, un poste de travail activé dans un pool automatisé avec des affectations dédiées n'est pas nécessairement disponible. Il n'est disponible que si le poste de travail n'est pas affecté à un utilisateur.

Tableau 5-26 décrit le pool automatisé d'affectation dédiée dans cet exemple.

Tableau 5-26. Exemple des paramètres de pool de postes de travail d'un pool automatisé avec des affectations dédiées

Paramètre du pool de postes de travail	Valeur
Number of desktops (minimum) (Nombre de postes de travail (minimum))	3
Number of desktops (maximum) (Nombre de postes de travail (maximum))	5
Number of spare, powered-on desktops (Nombre de postes de travail de rechange activés)	2
Remote desktop power policy (Règle d'alimentation de poste de travail distant)	Ensure desktops are always powered on (S'assurer que les postes de travail sont toujours activés)

Quand ce pool de postes de travail est approvisionné, 3 postes de travail sont créés et activés. Si les postes de travail sont désactivés dans vCenter Server, ils sont immédiatement réactivés, en fonction de la règle d'alimentation.

Lorsqu'un utilisateur se connecte à un poste de travail dans le pool, le poste de travail lui est affecté de façon permanente. Lorsqu'il s'en déconnecte, le poste de travail n'est plus disponible pour les autres utilisateurs. Toutefois, la règle **[Ensure desktops are always powered on (S'assurer que les postes de travail sont toujours activés)]** s'applique toujours. Si le poste de travail affecté est désactivé dans vCenter Server, il se rallume immédiatement.

Lorsqu'un autre utilisateur se connecte, un deuxième poste de travail est affecté. Comme le nombre de postes de travail de rechange est inférieur à la limite quand le deuxième utilisateur se connecte, un autre poste de travail est créé et activé. Un poste de travail supplémentaire est créé et activé chaque fois qu'un nouvel utilisateur est affecté jusqu'à ce que la limite de poste de travail maximale soit atteinte.

Éviter les conflits de règle d'alimentation de View

Lorsque vous utilisez View Administrator pour configurer une règle d'alimentation, vous devez comparer la règle d'alimentation aux paramètres dans le panneau de configuration Options d'alimentation du système d'exploitation client pour éviter les conflits de règle d'alimentation.

Un poste de travail View peut devenir temporairement inaccessible si la règle d'alimentation configurée pour le poste de travail de machine virtuelle n'est pas compatible avec une option d'alimentation configurée pour le système d'exploitation client. S'il y a d'autres postes de travail dans le même pool, ils peuvent également être affectés.

La configuration suivante est un exemple de conflit de règle d'alimentation :

- Dans View Administrator, la règle d'alimentation **[Suspend (Interrompre)]** est configurée pour le poste de travail de machine virtuelle. Cette règle force la machine virtuelle à s'interrompre lorsqu'elle n'est pas utilisée.
- Dans le panneau de configuration Options d'alimentation du système d'exploitation client, l'option **[Put the Computer to sleep (Mettre l'ordinateur en veille)]** est définie sur trois minutes.

Dans cette configuration, View Connection Server et le système d'exploitation client peuvent interrompre la machine virtuelle. L'option d'alimentation du système d'exploitation client peut rendre la machine virtuelle indisponible lorsque View Connection Server s'attend à la voir activée.

Configurer View Storage Accelerator pour des pools de postes de travail

Vous pouvez configurer des pools de postes de travail afin de permettre aux hôtes ESXi de mettre en cache des données de disque de machine virtuelle. Cette fonction, appelée View Storage Accelerator, utilise la fonction CBRC (Content Based Read Cache) dans les hôtes ESXi. View Storage Accelerator peut réduire l'IOPS et améliorer les performances au cours de tempêtes de démarrage, lorsque plusieurs postes de travail démarrent ou exécutent des analyses antivirus simultanément. La fonction est également utile lorsque des administrateurs ou des utilisateurs chargent des applications ou des données fréquemment. Pour utiliser cette fonction, vous devez vérifier que View Storage Accelerator est activé pour les pools de postes de travail individuels.

View Storage Accelerator est activé pour un pool par défaut. Vous pouvez activer ou désactiver View Storage Accelerator lorsque vous créez ou modifiez un pool.

Vous pouvez activer View Storage Accelerator sur des pools contenant des clones liés et sur des pools contenant des machines virtuelles complètes.

View Storage Accelerator est également pris en charge avec le mode local. Les utilisateurs peuvent emprunter des postes de travail dans des pools activés pour View Storage Accelerator. La fonction est désactivée lorsqu'un poste de travail est emprunté et réactivé lorsque le poste de travail est restitué.

La technologie de snapshot NFS natif (VAAI) n'est pas prise en charge dans les pools activés pour View Storage Accelerator.

View Storage Accelerator est maintenant conçu pour fonctionner dans des configurations qui utilisent la hiérarchisation de réplica View, dans lesquelles des réplicas sont stockés dans un magasin de données séparé des clones liés. Bien que les avantages de performance de l'utilisation de View Storage Accelerator avec la hiérarchisation de réplica View ne soient pas matériellement importants, certains avantages liés à la capacité peuvent être atteints en stockant les réplicas sur un magasin de données séparé. Par conséquent, cette combinaison est testée et prise en charge.

Lorsqu'une machine virtuelle est créée, View indexe le contenu de chaque fichier de disque virtuel. Les index sont stockés dans un fichier condensé de machine virtuelle. Au moment de l'exécution, l'hôte ESXi lit les fichiers condensés et met en cache les blocs de données communs dans la mémoire. Pour maintenir le cache de l'hôte ESXi à jour, View régénère les fichiers condensés à des intervalles spécifiés et lorsque la machine virtuelle est recomposée. Vous pouvez modifier l'intervalle de régénération.

Prérequis

- Vérifiez que vos hôtes vCenter Server et ESXi sont les versions 5.0 ou supérieures.

  Dans un cluster ESXi, vérifiez que la version de tous les hôtes est la version 5.0 ou supérieure.

- Vérifiez que l'utilisateur de vCenter Server s'est vu affecté le privilège **Général > Agir comme vCenter Server** dans vCenter Server. Consultez les rubriques dans la documentation *Installation de VMware Horizon View* qui décrivent les privilèges de View Manager et de View Composer requis pour l'utilisateur de vCenter Server.

- Vérifiez que View Storage Accelerator est activé dans vCenter Server. Reportez-vous à la section « Configurer View Storage Accelerator pour vCenter Server », page 21.

Procédure

1 Dans View Administrator, affichez la page Options de stockage avancées.

Option	Description
Nouveau pool de postes de travail	Démarrez l'assistant Ajouter un pool pour commencer la création d'un pool de postes de travail automatisé. Suivez les invites de configuration de l'assistant jusqu'à la page Options de stockage avancées.
Pool de postes de travail existant	Sélectionnez le pool existant, cliquez sur **[Modifier]** et cliquez sur l'onglet **[Options de stockage avancées]** . Dans un pool existant, les fichiers condensés de View Storage Accelerator ne sont pas configurés pour les machines virtuelles tant qu'elles sont activées.

2 Pour activer View Storage Accelerator pour le pool, vérifiez que la case **[Utiliser View Storage Accelerator]** est cochée.

Ce paramètre est sélectionné par défaut. Pour désactiver le paramètre, décochez la case **[Utiliser View Storage Accelerator]** .

3 (Facultatif) Spécifiez les types de disque à mettre en cache en sélectionnant **[Disques du système d'exploitation]** uniquement ou **[Disques du système d'exploitation et persistants]** dans le menu.

[Disques du système d'exploitation] est sélectionné par défaut.

Si vous configurez View Storage Accelerator pour des machines virtuelles complètes, vous ne pouvez pas sélectionner un type de disque. View Storage Accelerator est exécuté sur toute la machine virtuelle.

4 (Facultatif) Dans la zone de texte **[Régénérer l'accélérateur de stockage après]** , spécifiez l'intervalle, en jours, après lequel se produit la régénération des fichiers condensés de View Storage Accelerator.

L'intervalle de régénération par défaut est de 7 jours.

Suivant

Vous pouvez configurer des jours et des heures d'interruption durant lesquels la récupération d'espace disque et la régénération de View Storage Accelerator n'ont pas lieu. Reportez-vous à la section « Définir des heures d'interruption pour des opérations ESXi sur des postes de travail View », page 132.

Définir des heures d'interruption pour des opérations ESXi sur des postes de travail View

La régénération des fichiers condensés pour View Storage Accelerator et la récupération de l'espace disque de machine virtuelle peuvent utiliser des ressources ESXi. Pour vous assurer que des ressources ESXi sont dédiées à des tâches de premier plan lorsque cela est nécessaire, vous pouvez empêcher les hôtes ESXi d'exécuter ces opérations pendant des périodes de temps spécifiées certains jours.

Par exemple, vous pouvez spécifier une période d'interruption tous les matins du lundi au vendredi, lorsque les utilisateurs commencent à travailler. Des tempêtes de démarrage et des tempêtes d'E/S d'analyse antivirus ont lieu. Vous pouvez spécifier différentes heures d'interruption selon les jours.

La récupération d'espace disque et la régénération des fichiers condensés de View Storage Accelerator n'ont pas lieu lors des heures d'interruption que vous avez définies. Vous ne pouvez pas définir des heures d'interruption séparées pour chaque opération.

View permet aux fichiers condensés de View Storage Accelerator d'être créés pour les nouveaux postes de travail lors de l'étape d'approvisionnement, même lorsqu'une heure d'interruption est effective.

Prérequis

- Vérifiez que **[Activer View Storage Accelerator]** , **[Activer la récupération d'espace]** ou les deux fonctions sont sélectionnées pour vCenter Server.

- Vérifiez que **[Utiliser View Storage Accelerator]** , **[Récupérer l'espace disque de machine virtuelle]** ou les deux fonctions sont sélectionnées pour le pool de postes de travail.

Procédure

1 Sur la page Options de stockage avancées de l'assistant Ajouter un pool, allez à **[Durée d'interruption]** et cliquez sur **[Ajouter]** .

Si vous modifiez un pool existant, cliquez sur l'onglet **[Options de stockage avancées]** .

2 Cochez les jours d'interruption et spécifiez les heures de début et de fin.

Le sélecteur horaire utilise une horloge de 24 heures. Par exemple, 10:00 correspond à 10:00 a.m. et 22:00 à 10:00 p.m.

3 Cliquez sur **[OK]** .

4 Pour ajouter une autre période d'interruption, cliquez sur **[Ajouter]** et spécifiez une autre période.

5 Pour modifier ou supprimer une période d'interruption, sélectionnez la période dans la liste Heures d'interruption et cliquez sur **[Modifier]** ou **[Supprimer]** .

Déploiement de pools de postes de travail volumineux

Lorsque de nombreux utilisateurs requièrent la même image de poste de travail, vous pouvez créer un pool automatisé volumineux à partir d'un modèle ou d'une machine virtuelle parente. En utilisant une seule image de base et un seul nom de pool, vous pouvez éviter de diviser les postes de travail arbitrairement en plus petits groupes qui doivent être gérés séparément. Cette stratégie simplifie vos tâches de déploiement et d'administration de View.

Pour prendre en charge des pools volumineux, vous pouvez créer des pools sur des clusters ESXi contenant jusqu'à 32 hôtes ESXi. Vous pouvez également configurer un pool pour qu'il utilise plusieurs étiquettes de réseau, en rendant les adresses IP de plusieurs groupes de ports disponibles pour les machines virtuelles de poste de travail.

Configuration de pools sur des clusters avec plus de huit hôtes

Dans vSphere 5.1 et supérieur, vous pouvez déployer un pool de postes de travail de clone lié sur un cluster contenant jusqu'à 32 hôtes ESXi. La version de tous les hôtes ESXi dans le cluster doit être la version 5.1 ou supérieure. Les hôtes peuvent utiliser des magasins de données VMFS ou NFS. La version des magasins de données VMFS doit être VMFS5 ou supérieur.

Dans vSphere 5.0, vous pouvez déployer des clones liés sur un cluster contenant plus de huit hôtes ESXi, mais vous devez stocker les disques de réplica sur des magasins de données NFS. Vous pouvez stocker des disques de réplica sur des magasins de données VMFS uniquement avec des clusters qui contiennent huit hôtes ou moins.

Dans vSphere 5.0, les règles suivantes s'appliquent lorsque vous configurez un pool de clone lié sur un cluster contenant plus de huit hôtes :

- Si vous stockez des disques de réplica sur les mêmes magasins de données que les disques du système d'exploitation, vous devez stocker les disques de réplica et du système d'exploitation sur des magasins de données NFS.
- Si vous stockez des disques de réplica sur des magasins de données séparés des disques du système d'exploitation, les disques de réplica doivent être stockés sur des magasins de données NFS. Les disques du système d'exploitation peuvent être stockés sur des magasins de données NFS ou VMFS.

- Si vous stockez des disques persistants de View Composer sur des magasins de données séparés, les disques persistants peuvent être configurés sur des magasins de données NFS ou VMFS.

Dans vSphere 4.1 et versions antérieures, vous pouvez déployer des pools de postes de travail uniquement avec des clusters contenant huit hôtes ou moins.

Affectation de plusieurs étiquettes de réseau à un pool de postes de travail

Dans View 5.5 et versions supérieures, vous pouvez configurer un pool automatisé pour utiliser plusieurs étiquettes de réseau. Vous pouvez affecter plusieurs étiquettes de réseau à un pool de clone lié ou un pool automatisé contenant des machines virtuelles complètes.

Dans les versions précédentes, les machines virtuelles dans le pool héritaient des étiquettes de réseau qui étaient utilisées par les cartes réseau sur la machine virtuelle parente ou le modèle. Une machine virtuelle parente ou un modèle classique contient une carte réseau et une étiquette de réseau. Une étiquette de réseau définit un groupe de ports et un VLAN. En général, le masque de réseau d'un VLAN fournit une plage limitée d'adresses IP disponibles.

Dans View 5.5 et versions supérieures, vous pouvez affecter des étiquettes de réseau disponibles dans vCenter Server pour tous les hôtes ESXi dans le cluster sur lequel le pool de postes de travail est déployé. En configurant plusieurs étiquettes de réseau pour le pool, vous augmentez considérablement le nombre d'adresses IP pouvant être affectées aux machines virtuelles dans le pool.

Vous devez utiliser des cmdlets View PowerCLI pour affecter plusieurs étiquettes de réseau à un pool. Vous ne pouvez pas effectuer cette tâche dans View Administrator.

Pour plus d'informations sur l'utilisation de View PowerCLI pour effectuer cette tâche, consultez la section « Affecter plusieurs étiquettes de réseau à un pool de postes de travail » dans le chapitre « Utilisation de View PowerCLI » dans le document *Intégration de VMware Horizon View*.

Autorisation d'utilisateurs et de groupes 6

Vous configurez des autorisations de pool de postes de travail pour contrôler les postes de travail View auxquels vos utilisateurs peuvent accéder. Vous pouvez également configurer la fonction d'autorisations limitées pour contrôler l'accès en fonction de l'instance de View Connection Server à laquelle les utilisateurs se connectent lorsqu'ils sélectionnent des postes de travail.

Ce chapitre aborde les rubriques suivantes :

Ajouter des autorisations à des pools de postes de travail

Avant que les utilisateurs puissent accéder à un poste de travail View, ils doivent être autorisés à utiliser un pool de postes de travail.

Prérequis

Créez un pool de postes de travail. Reportez-vous à la section Chapitre 5, « Création de pools de postes de travail », page 97.

Procédure

1 Dans View Administrator, sélectionnez **[Inventory (Inventaire)] > [Pools]** .

2 Sélectionnez le pool de postes de travail et cliquez sur **[Entitlements (Autorisations)]** .

3 Cliquez sur **[Add (Ajouter)]** , sélectionnez un ou plusieurs critères de recherche, puis cliquez sur **[Find (Rechercher)]** pour rechercher des utilisateurs ou des groupes en fonction de vos critères de recherche.

Remarque Les groupes locaux de domaine sont filtrés dans les résultats de recherche pour des domaines en mode mixte. Vous ne pouvez pas autoriser des utilisateurs dans des groupes locaux de domaine si votre domaine est configuré en mode mixte.

---

4 Sélectionnez les utilisateurs ou les groupes pour lesquels vous voulez autoriser l'accès aux postes de travail dans le pool et cliquez sur **[OK]** .

5 Cliquez sur **[OK]** pour enregistrer vos modifications.

Supprimer des autorisations d'un pool de postes de travail

Vous pouvez supprimer des autorisations d'un pool de postes de travail pour empêcher des utilisateurs ou des groupes spécifiques d'accéder à un poste de travail.

Procédure

1 Dans View Administrator, sélectionnez **[Inventory (Inventaire)]** > **[Pools]** .

2 Sélectionnez le pool de postes de travail et cliquez sur **[Entitlements (Autorisations)]** .

3 Sélectionnez l'utilisateur ou le groupe pour lequel vous souhaitez supprimer l'autorisation et cliquez sur **[Remove (Supprimer)]** .

4 Cliquez sur **[OK]** pour enregistrer vos modifications.

Consulter des autorisations de pool de postes de travail

Vous pouvez consulter les pools de postes de travail auxquels un utilisateur ou un groupe est autorisé à accéder.

Procédure

1 Dans View Administrator, sélectionnez **[Users and Groups (Utilisateurs et groupes)]** et cliquez sur le nom de l'utilisateur ou du groupe.

2 Sélectionnez l'onglet **[Summary (Résumé)]** .

Le volet Pool Entitlements (Autorisations de pool) répertorie les pools auxquels l'utilisateur ou le groupe est actuellement autorisé à accéder.

Restriction de l'accès aux postes de travail View

Vous pouvez également configurer la fonction d'autorisations limitées pour limiter l'accès au poste de travail View en fonction de l'instance de View Connection Server à laquelle les utilisateurs se connectent lorsqu'ils sélectionnent des postes de travail.

Avec des autorisations limitées, vous affectez une ou plusieurs balises à une instance de View Connection Server. Ensuite, lorsque vous configurez un pool de postes de travail, vous sélectionnez les balises des instances de View Connection Server que vous voulez rendre capables d'accéder au pool de postes de travail.

Lorsque les utilisateurs ouvrent une session via une instance marquée de View Connection Server, ils ne peuvent accéder qu'à ces pools de postes de travail qui ont au moins une balise correspondante ou qui n'ont aucune balise.

- Exemple d'autorisation limitée page 173

  Cet exemple montre un déploiement de View comportant deux instances de View Connection Server. La première instance prend en charge les utilisateurs internes. La deuxième instance est couplée avec un serveur de sécurité et prend en charge les utilisateurs externes.

- Correspondance de balise page 174

  La fonction d'autorisations limitées utilise la correspondance de balise pour déterminer si une instance de View Connection Server peut accéder à un pool de postes de travail particulier.

- Considérations et limites des autorisations limitées page 174

  Avant d'implémenter des autorisations limitées, vous devez connaître certaines considérations et limites.

- Affecter une balise à une instance de View Connection Server page 175

  Lorsque vous affectez une balise à une instance de View Connection Server, les utilisateurs qui se connectent à ce serveur View Connection Server ne peuvent accéder qu'aux pools de postes de travail qui ont une balise correspondante ou aucune balise.

- Affecter une balise à un pool de postes de travail page 175

  Lorsque vous affectez une balise à un pool de postes de travail, seuls les utilisateurs qui se connectent à une instance de View Connection Server ayant une balise correspondante peuvent accéder aux postes de travail de ce pool.

Exemple d'autorisation limitée

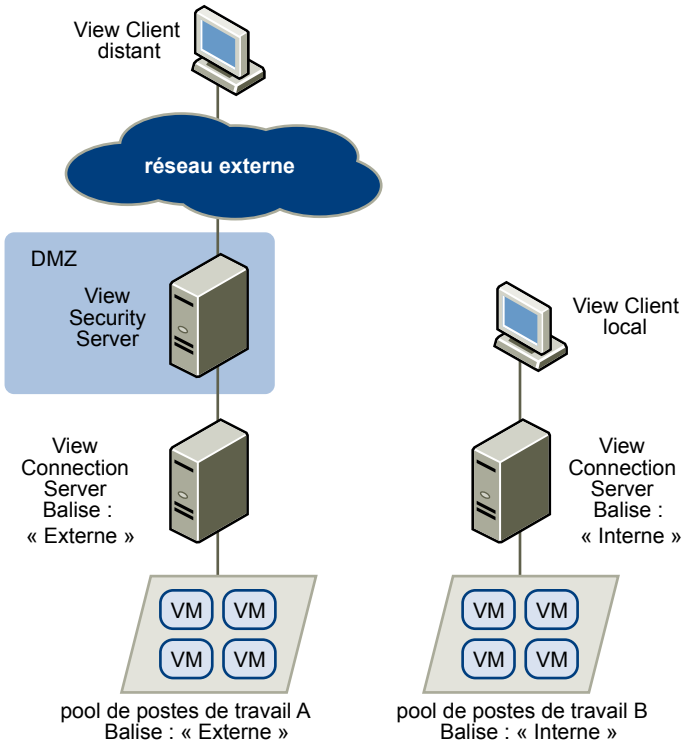
Cet exemple montre un déploiement de View comportant deux instances de View Connection Server. La première instance prend en charge les utilisateurs internes. La deuxième instance est couplée avec un serveur de sécurité et prend en charge les utilisateurs externes.

Pour empêcher les utilisateurs externes d'accéder à certains postes de travail, vous pouvez configurer des autorisations limitées comme suit :

- Affectez la balise « Internal » à l'instance de View Connection Server qui prend en charge les utilisateurs internes.
- Affectez la balise « External » à l'instance de View Connection Server qui est couplée avec le serveur de sécurité et qui prend en charge les utilisateurs externes.
- Affectez la balise « Internal » aux pools de postes de travail auxquels ne doivent accéder que les utilisateurs internes.
- Affectez la balise « External » aux pools de postes de travail auxquels ne doivent accéder que les utilisateurs externes.

Les utilisateurs externes ne peuvent pas voir les pools de postes de travail marqués comme « Internal » car ils ouvrent une session via le serveur View Connection Server marqué comme « External ». Les utilisateurs internes ne peuvent pas voir les pools de postes de travail marqués comme « External » car ils ouvrent une session via le serveur View Connection Server marqué comme « Internal ». Figure 6-1 illustre cette configuration.

Figure 6-1. Configuration d'une autorisation limitée



Vous pouvez également utiliser des autorisations limitées pour contrôler l'accès à des postes de travail en fonction de la méthode d'authentification utilisateur que vous configurez pour une instance de View Connection Server particulière. Par exemple, vous pouvez rendre certains pools de postes de travail disponibles pour des utilisateurs qui se sont authentifiés avec une carte à puce.

Correspondance de balise

La fonction d'autorisations limitées utilise la correspondance de balise pour déterminer si une instance de View Connection Server peut accéder à un pool de postes de travail particulier.

Au niveau le plus basique, la correspondance de balise détermine qu'une instance de View Connection Server avec une balise spécifique peut accéder à un pool de postes de travail qui a la même balise.

L'absence d'affectation de balise peut également affecter si une instance de View Connection Server peut accéder à un pool de postes de travail. Par exemple, des instances de View Connection Server qui ne contiennent aucune balise ne peuvent accéder qu'à des pools de postes de travail qui ne contiennent aucune balise.

Tableau 6-1 montre comment la fonction d'autorisations limitées détermine quand un serveur View Connection Server peut accéder à un pool de postes de travail.

Tableau 6-1. Règles de correspondance de balise

View Connection Server	Pool de postes de travail	Accès autorisé ?
Pas de balise	Pas de balise	Oui
Pas de balise	Une ou plusieurs balises	Non
Une ou plusieurs balises	Pas de balise	Oui
Une ou plusieurs balises	Une ou plusieurs balises	Uniquement quand les balises correspondent

La fonction d'autorisations limitées ne fait qu'appliquer la correspondance de balise. Vous devez concevoir votre topologie de réseau pour forcer certains clients à se connecter via une instance de View Connection Server particulière.

Considérations et limites des autorisations limitées

Avant d'implémenter des autorisations limitées, vous devez connaître certaines considérations et limites.

- Une instance de Serveur de connexion View ou un pool de postes de travail peut contenir plusieurs balises.
- Plusieurs instances de Serveur de connexion View et pools de postes de travail peuvent avoir la même balise.
- Des pools de postes de travail qui ne contiennent aucune balise peuvent être accédés par n'importe quelle instance de Serveur de connexion View.
- Des instances de Serveur de connexion View qui ne contiennent aucune balise ne peuvent accéder qu'à des pools de postes de travail qui ne contiennent aucune balise.
- Si vous utilisez un serveur de sécurité, vous devez configurer des autorisations limitées sur l'instance de Serveur de connexion View à laquelle le serveur de sécurité est couplé. Vous ne pouvez pas configurer des autorisations limitées sur un serveur de sécurité.
- Vous ne pouvez pas modifier ou supprimer une balise d'une instance de Serveur de connexion View si cette balise est toujours affectée à un pool de postes de travail et qu'aucune autre instance n'a de balise correspondante.
- Les autorisations limitées sont prioritaires par rapport aux autres autorisations de poste de travail. Par exemple, même si un utilisateur est autorisé à accéder à un poste de travail particulier, l'utilisateur ne pourra pas accéder à celui-ci si la balise du pool de postes de travail ne correspond pas à la balise affectée à l'instance de Serveur de connexion View à laquelle l'utilisateur est connecté.

- Si vous prévoyez de fournir l'accès à vos postes de travail via Horizon Workspace, et si vous configurez des restrictions de Serveur de connexion View, Horizon User Portal peut afficher les postes de travail aux utilisateurs lorsque ces postes de travail sont en fait limités. Lorsqu'un utilisateur Horizon tente d'ouvrir une session sur un poste de travail, elle ne se lancera pas si la balise du pool de postes de travail ne correspond pas à la balise affectée à l'instance de Serveur de connexion View à laquelle l'utilisateur est connecté.

Affecter une balise à une instance de View Connection Server

Lorsque vous affectez une balise à une instance de View Connection Server, les utilisateurs qui se connectent à ce serveur View Connection Server ne peuvent accéder qu'aux pools de postes de travail qui ont une balise correspondante ou aucune balise.

Procédure

1 Dans View Administrator, sélectionnez **[View Configuration (Configuration de View)] > [Servers (Serveurs)]** .

2 Dans View Connection Servers (Serveurs View Connection Server), sélectionnez l'instance de View Connection Server et cliquez sur **[Edit (Modifier)]** .

3 Saisissez une ou plusieurs balises dans le champ **[Tags (Balises)]** .

Séparez les balises avec une virgule ou un point-virgule.

4 Cliquez sur **[OK]** pour enregistrer vos modifications.

Suivant

Affectez la balise à des pools de postes de travail.

Affecter une balise à un pool de postes de travail

Lorsque vous affectez une balise à un pool de postes de travail, seuls les utilisateurs qui se connectent à une instance de View Connection Server ayant une balise correspondante peuvent accéder aux postes de travail de ce pool.

Vous pouvez affecter une balise quand vous ajoutez ou modifiez un pool de postes de travail.

Prérequis

Affectez des balises à une ou plusieurs instances de View Connection Server.

Procédure

1 Dans View Administrator, sélectionnez **[Inventory (Inventaire)] > [Pools]** .

2 Sélectionnez le pool auquel vous souhaitez affecter une balise.

Option	Action
Affecter une balise à un nouveau pool	Cliquez sur **[Add (Ajouter)]** pour démarrer l'assistant Add Pool (Ajouter un pool), puis définissez et identifiez le pool.
Affecter une balise à un pool existant	Sélectionnez le pool et cliquez sur **[Edit (Modifier)]** .

3 Allez à la page Pool Settings (Paramètres de pool).

Option	Action
Paramètres de pool pour un nouveau pool	Cliquez sur **[Pool Settings (Paramètres de pool)]** dans l'assistant Add Pool (Ajouter un pool).
Paramètres de pool pour un pool existant	Sélectionnez l'onglet **[Pool Settings (Paramètres de pool)]** .

4 Cliquez sur **[Browse (Parcourir)]** à côté de **[Connection Server restrictions (Restrictions de Connection Server)]** et configurez les instances de View Connection Server pouvant accéder au pool de postes de travail.

Option	Action
Rendre le pool accessible à n'importe quelle instance de View Connection Server	Sélectionnez **[No Restrictions (Aucune restriction)]** .
Rendre le pool accessible uniquement à des instances de View Connection Server possédant ces balises	Sélectionnez **[Restrict to these tags (Limiter à ces balises)]** et sélectionnez une ou plusieurs balises. Vous pouvez utiliser les cases à cocher pour sélectionner plusieurs balises.

5 Cliquez sur **[OK]** pour enregistrer vos modifications.

Configuration de l'authentification utilisateur 7

View utilise votre infrastructure Active Directory existante pour l'authentification et la gestion des utilisateurs. Pour renforcer la sécurité, vous pouvez intégrer View à des solutions d'authentification par carte à puce et d'authentification à deux facteurs, telles que RSA SecurID et RADIUS.

Ce chapitre aborde les rubriques suivantes :

Utilisation de l'authentification SAML 2.0

L'authentification de serveur SAML (Security Assertion Markup Language) permet à View d'échanger des informations d'authentification avec d'autres services, tels que le service Horizon Web. Lorsqu'un utilisateur se connecte à Horizon Workspace, l'authentification de serveur SAML lui permet d'initier une session View et de commencer à utiliser le poste de travail virtuel sans être invité à fournir de nouveau des informations d'identification à la connexion.

L'authentification à View est gérée par le service Horizon via l'authentificateur SAML 2.0. Lorsque la délégation d'authentification est activée, et qu'un utilisateur est vérifié par SAML, le fournisseur d'identité SAML exécute toutes les authentifications, à l'exception de la clause de non-responsabilité.

Lorsque vous sélectionnez une icône de poste de travail View dans Horizon User Portal, un artefact SAML est généré. Le View Client envoie l'artefact à Serveur de connexion View. Lorsque Serveur de connexion View valide l'artefact, il se connecte avec Horizon Workspace.

Serveur de connexion View envoie l'artefact à Horizon, où il est validé. Horizon Workspace envoie ensuite une assertion SAML à Serveur de connexion View, qui est validée et authentifie l'utilisateur avec View. Cette authentification est utilisée pour lancer le poste de travail View après la validation. L'assertion est générée par Horizon Workspace après la réception de l'artefact de la part de Serveur de connexion View. Le Serveur de connexion View valide l'assertion reçue d'Horizon Workspace.

Vous devez associer le Serveur de connexion View à un service d'authentification SAML, tel qu'Horizon Workspace, pour faciliter ce processus.

Remarque Si vous prévoyez de fournir l'accès à vos postes de travail via Horizon Workspace, vérifiez que vous créez les pools de postes de travail en tant qu'utilisateur avec des autorisations Administrateurs dans le dossier racine dans View. Si vous accordez à l'utilisateur des autorisations Administrateurs sur un dossier autre que le dossier racine, Horizon Workspace ne reconnaîtra pas l'authentificateur SAML 2.0 que vous configurez dans View et vous ne pouvez pas configurer le pool dans Horizon Workspace.

Configurer des authentificateurs SAML 2.0 dans View Administrator

Pour configurer un serveur SAML afin qu'il effectue des tâches d'authentification, vous devez ajouter un authentificateur SAML et spécifier une étiquette, l'URL de métadonnées, l'URL d'administration et d'autres paramètres.

Prérequis

- Vérifiez que l'authentificateur SAML 2.0 est installé et disponible pour son inclusion dans le service Horizon et Serveur de connexion View. Pour plus d'informations sur l'installation et la configuration, rendez-vous sur https://www.vmware.com/support/pubs/horizon_pubs.html.
- Notez le nom du serveur Horizon. Vous devez entrer ce nom dans la chaîne de l'URL de métadonnées lors de la configuration.
- Notez l'URL pour accéder à la console d'administration du fournisseur d'identité SAML. Vous spécifiez cette URL lors de la configuration.

Procédure

1 Dans View Administrator, allez à **[Configuration de View > Serveurs]** .

2 Cliquez sur l'onglet **[Serveurs de connexion]** .

3 Sélectionnez un serveur et cliquez sur **[Modifier]** .

4 Cliquez sur l'onglet **[Authentification]** dans la boîte de dialogue **[Modifier les paramètres du Serveur de connexion View]** .

5 Dans le menu déroulant **[Délégation de l'authentification à VMware Horizon (authentificateur SAML 2.0)]** , sélectionnez le paramètre d'authentification approprié.

Option	Description
Désactivée	L'authentification SAML est désactivée.
Autorisé	L'authentification SAML est autorisée. Vous pouvez vous connecter à View manuellement à partir de View Client ou à l'aide de Horizon.
Requise	L'authentification SAML est requise. Vous pouvez vous connecter à View uniquement à partir de Horizon. Vous ne pouvez pas vous connecter manuellement.

6 Dans le menu déroulant **[Authentificateur SAML]** , sélectionnez **[Créer un nouvel authentificateur]** .

Si un authentificateur SAML 2.0 a déjà été ajouté, cliquez sur **[Gérer des authentificateurs] > [Ajouter un authentificateur SAML 2.0]** .

7 Complétez les informations dans la boîte de dialogue **[Ajouter un authentificateur SAML 2.0]** .

Option	Description
Étiquette	Utilisée pour identifier l'authentificateur SAML 2.0 dans le menu déroulant **[Sélectionner un authentificateur]** dans l'onglet **[Authentificateurs]** de la boîte de dialogue **[Modifier les paramètres du Serveur de connexion View]** .
Description	Cette option est facultative. Il s'agit d'une courte description de l'authentificateur.
URL de métadonnées	Utilisée pour récupérer toutes les informations requises afin d'échanger des informations SAML entre le fournisseur d'identité SAML et un serveur de connexion. L'URL est au format suivant : https://*NOM DE VOTRE SERVEUR HORIZON*/SAAS/API/1.0/GET/metadata/idp.xml.
URL d'administration	Cette option est facultative. Cette URL est un lien vers la console d'administration du fournisseur d'identité SAML.

8 Cliquez sur **[OK]** .

Si vous ne disposez d'aucun certificat approuvé valide, vous serez invité à vérifier le certificat.

9 Allez à **[Tableau de bord]** dans la section Inventaire de View Administrator.

10 Cliquez sur **[Authentificateurs SAML 2.0]** .

11 Sélectionnez le serveur SAML que vous avez modifié ou ajouté, vérifiez les détails et cliquez sur **[OK]** .

Le tableau de bord View affiche désormais l'authentificateur SAML 2.0 avec une condition d'intégrité, qui est indiquée par une icône verte.

Vous pouvez configurer chaque instance de Serveur de connexion View avec un paramètre d'authentification **[Requis]** , **[Autorisé]** ou **[Désactivé]** , en fonction des exigences spécifiques du client.

Utilisation de l'authentification par carte à puce

Vous pouvez configurer une instance de Serveur de connexion View ou un serveur de sécurité pour que les utilisateurs d'un poste de travail View puissent s'authentifier à l'aide d'une carte à puce. Les cartes à puce sont parfois appelées Common Access Card (CAC).

Une carte à puce est une petite carte plastique qui contient une puce informatique. La puce, qui est semblable à un ordinateur miniature, inclut un stockage sécurisé de données, y compris des clés privées et des certificats de clé publique.

Avec l'authentification par carte à puce, un utilisateur insère une carte à puce dans un lecteur de carte à puce fixé sur l'ordinateur client et il saisit un code PIN. L'authentification par carte à puce fournit une authentification à deux facteurs en vérifiant ce que l'utilisateur possède (la carte à puce) et ce que l'utilisateur sait (le code PIN).

Pour plus d'informations sur les exigences matérielles et logicielles pour la mise en œuvre de l'authentification par carte à puce, consultez le document *Installation de VMware Horizon View*. Le site Web Microsoft TechNet comporte des informations détaillées sur la planification et l'implémentation de l'authentification par carte à puce pour les systèmes Windows.

L'authentification par carte à puce n'est pas prise en charge par View Client pour Mac ou View Administrator. Pour plus d'informations sur la prise en charge des cartes à puce, consultez le document *Planification de l'architecture de VMware Horizon View*.

Ouverture de session avec une carte à puce

Lorsqu'un utilisateur insère une carte à puce dans un lecteur de carte à puce, les certificats utilisateur sur la carte à puce sont copiés dans le magasin de certificats local sur le système client. Les certificats dans le magasin de certificats local sont disponibles pour toutes les applications exécutées sur l'ordinateur client, y compris l'application du client View.

Lorsqu'un utilisateur initie une connexion sur une instance de Serveur de connexion View ou un serveur de sécurité configuré pour l'authentification par carte à puce, l'instance de Serveur de connexion View ou le serveur de sécurité envoie une liste d'autorités de certification approuvées au client View. Le client View compare cette liste aux certificats utilisateur disponibles, sélectionne un certificat approprié et invite l'utilisateur à saisir un code PIN de carte à puce. Si plusieurs certificats utilisateur sont valides, le client View invite l'utilisateur à sélectionner un certificat.

Le client View envoie le certificat utilisateur à l'instance de Serveur de connexion View ou au serveur de sécurité, qui vérifie le certificat en contrôlant la confiance du certificat et la période de validité. En général, les utilisateurs peuvent s'authentifier si leur certificat utilisateur est signé et valide. Si la vérification de la révocation des certificats est configurée, les utilisateurs qui ont des certificats utilisateur révoqués ne peuvent pas s'authentifier.

Le changement du protocole d'affichage n'est pas pris en charge avec l'authentification par carte à puce. Pour modifier les protocoles d'affichage après une authentification par carte à puce, un utilisateur doit fermer puis rouvrir la session.

Ouverture de session sur des postes de travail locaux avec l'authentification par carte à puce hors ligne

Avec l'authentification par carte à puce hors ligne, les utilisateurs peuvent ouvrir une session sur un poste de travail local avec une carte à puce lorsque le poste de travail n'est pas connecté à View Connection Server.

Pour utiliser l'authentification par carte à puce hors ligne, les utilisateurs doivent utiliser la même méthode d'authentification que celle qu'ils ont utilisée pour s'authentifier sur View Connection Server lors de leur dernière ouverture de session. Par exemple, si un utilisateur a ouvert une session avec la carte à puce A, puis de nouveau avec l'authentification par mot de passe, et finalement ouvre une session avec la carte à puce B, l'utilisateur doit alors utiliser la carte à puce B pour s'authentifier avec l'authentification par carte à puce hors ligne.

La valeur la plus récente de la règle de retrait de carte à puce est renforcée lors de l'authentification par carte à puce hors ligne. La règle de retrait de carte à puce détermine si les utilisateurs doivent se réauthentifier pour pouvoir accéder à leurs postes de travail après avoir retiré leurs cartes à puce. Si la règle est définie sur Disconnect user sessions on smart card removal (Déconnecter les sessions utilisateur lors du retrait de la carte à puce), le système d'exploitation client dans le poste de travail View est verrouillé lorsque les utilisateurs retirent leur carte à puce. La fenêtre de View Client reste ouverte, et les utilisateurs peuvent sélectionner **[Options] > [Send Ctrl-Alt-Delete (Envoyer Ctrl-Alt-Suppr)]** pour se connecter de nouveau. La règle de retrait de carte à puce est un paramètre de View Connection Server.

Configurer l'authentification par carte à puce

Pour configurer l'authentification par carte à puce, vous devez obtenir un certificat racine et l'ajouter à un fichier du magasin d'approbations du serveur, modifier les propriétés de configuration de View Connection Server et configurer des paramètres d'authentification par carte à puce. En fonction de votre environnement particulier, vous devrez peut-être effectuer des étapes supplémentaires.

Procédure

1 Obtenir le certificat racine de l'autorité de certification page 181

Vous devez obtenir le certificat racine auprès de l'autorité de certification qui a signé les certificats sur les cartes à puce présentées par vos utilisateurs.

2 Exporter un certificat racine à partir d'un certificat utilisateur page 182

Si vous avez un certificat utilisateur signé par une autorité de certification ou une carte à puce qui en contient un, vous pouvez exporter le certificat racine s'il est approuvé par votre système.

3 Ajouter le certificat racine à un fichier du magasin d'approbations du serveur page 182

Vous devez ajouter le certificat racine pour tous les utilisateurs approuvés à un fichier du magasin d'approbations du serveur pour que les instances de Serveur de connexion View et les serveurs de sécurité puissent authentifier des utilisateurs de carte à puce et les connecter à leurs postes de travail View.

4 Modifier des propriétés de configuration de Serveur de connexion View page 183

Pour activer l'authentification par carte à puce, vous devez modifier les propriétés de configuration de Serveur de connexion View sur votre hôte de Serveur de connexion View ou du Serveur de sécurité.

5 Configurer des paramètres de carte à puce dans View Administrator page 184

Vous pouvez utiliser View Administrator pour spécifier des paramètres afin de s'adapter à différents scénarios d'authentification par carte à puce.

Obtenir le certificat racine de l'autorité de certification

Vous devez obtenir le certificat racine auprès de l'autorité de certification qui a signé les certificats sur les cartes à puce présentées par vos utilisateurs.

Si vous n'avez pas le certificat racine de l'autorité de certification qui a signé les certificats sur les cartes à puce présentées par vos utilisateurs, vous pouvez exporter un certificat racine à partir d'un certificat utilisateur signé par une autorité de certification ou d'une carte à puce qui en contient un. Reportez-vous à la section « Exporter un certificat racine à partir d'un certificat utilisateur », page 182.

Procédure

1 Obtenez le certificat racine à partir de l'une des sources suivantes.

- Un serveur Microsoft IIS exécutant les services de certificats Microsoft. Pour plus d'informations sur l'installation de Microsoft IIS, l'émission des certificats et leur distribution dans votre entreprise, consultez le site Web Microsoft TechNet.
- Le certificat racine public d'une autorité de certification approuvée. Il s'agit de la source la plus courante de certificat racine dans des environnements avec une infrastructure de carte à puce et une approche normalisée pour la distribution et l'authentification des cartes à puce.

2 Sélectionnez un certificat à utiliser pour l'authentification par carte à puce.

La chaîne de signature répertorie les autorités de signature. Généralement, le meilleur certificat à sélectionner est celui de l'autorité intermédiaire qui se trouve au-dessus du certificat utilisateur.

3 Vérifiez que l'autorité ne signe pas d'autres certificats sur la carte.

Suivant

Ajoutez le certificat racine à un fichier du magasin d'approbations du serveur. Reportez-vous à la section « Ajouter le certificat racine à un fichier du magasin d'approbations du serveur », page 182.

Exporter un certificat racine à partir d'un certificat utilisateur

Si vous avez un certificat utilisateur signé par une autorité de certification ou une carte à puce qui en contient un, vous pouvez exporter le certificat racine s'il est approuvé par votre système.

Procédure

1 Si le certificat utilisateur est sur une carte à puce, insérez la carte à puce dans le lecteur pour ajouter le certificat utilisateur à votre magasin personnel.

Si le certificat utilisateur n'apparaît pas dans votre magasin personnel, utilisez le logiciel du lecteur pour exporter le certificat utilisateur vers un fichier.

2 Dans Internet Explorer, sélectionnez **[Tools (Outils)]** > **[Internet Options (Options Internet)]** .

3 Sous l'onglet **[Content (Contenu)]** , cliquez sur **[Certificates (Certificats)]** .

4 Sous l'onglet **[Personal (Personnel)]** , sélectionnez le certificat que vous voulez utiliser et cliquez sur **[View (Affichage)]** .

Si le certificat utilisateur n'apparaît pas dans la liste, cliquez sur **[Import (Importer)]** pour l'importer manuellement à partir d'un fichier. Une fois le certificat importé, vous pouvez le sélectionner dans la liste.

5 Sous l'onglet **[Certification Path (Chemin d'accès de certification)]** , sélectionnez le certificat en haut de l'arborescence et cliquez sur **[View Certificate (Afficher le certificat)]** .

Si le certificat utilisateur est signé comme faisant partie d'une hiérarchie d'approbation, le certificat de signature peut être signé par un autre certificat de niveau plus élevé. Sélectionnez le certificat parent (celui qui est actuellement signé par le certificat utilisateur) comme votre certificat racine.

6 Sous l'onglet **[Details (Détails)]** , cliquez sur **[Copy to File (Copier dans un fichier)]** .

L'assistant Certificate Export (Exportation de certificat) apparaît.

7 Cliquez sur **[Next (Suivant)]** > **[Next (Suivant)]** et saisissez un nom et un emplacement pour le fichier que vous voulez exporter.

8 Cliquez sur **[Next (Suivant)]** pour enregistrer le fichier comme certificat racine dans l'emplacement spécifié.

Suivant

Ajoutez le certificat racine à un fichier du magasin d'approbations du serveur.

Ajouter le certificat racine à un fichier du magasin d'approbations du serveur

Vous devez ajouter le certificat racine pour tous les utilisateurs approuvés à un fichier du magasin d'approbations du serveur pour que les instances de Serveur de connexion View et les serveurs de sécurité puissent authentifier des utilisateurs de carte à puce et les connecter à leurs postes de travail View.

Prérequis

- Vous devez obtenir le certificat racine auprès de l'autorité de certification qui a signé les certificats sur les cartes à puce présentées par vos utilisateurs. Reportez-vous à la section « Obtenir le certificat racine de l'autorité de certification », page 181.
- Vérifiez que l'utilitaire `keytool` est ajouté au chemin d'accès du système sur votre hôte de Serveur de connexion View ou du serveur de sécurité. Pour plus d'informations, consultez le document *Installation de VMware Horizon View*.

Procédure

1 Sur votre hôte de Serveur de connexion View ou du serveur de sécurité, utilisez l'utilitaire `keytool` pour importer le certificat racine dans le fichier du magasin d'approbations du serveur.

Par exemple : **`keytool –import –alias`** ***`alias`*** **`–file`** ***`root_certificate`*** **`–keystore`** ***`truststorefile.key`***

Dans cette commande, *alias* est le nom unique non sensible à la casse d'une nouvelle entrée dans le fichier du magasin d'approbations, *root_certificate* est le certificat racine que vous avez obtenu ou exporté, et *truststorefile.key* est le nom de fichier du magasin d'approbations auquel vous ajoutez le certificat racine. Si le fichier n'existe pas, il est créé dans le répertoire actuel.

Remarque L'utilitaire `keytool` peut vous inviter à créer un mot de passe pour le fichier du magasin d'approbations. Vous serez invité à fournir ce mot de passe si vous devez ajouter ultérieurement des certificats supplémentaires au fichier du magasin d'approbations.

2 Copiez le fichier du magasin d'approbations dans le dossier de configuration de la passerelle SSL sur l'hôte de Serveur de connexion View ou l'hôte du serveur de sécurité.

Par exemple : *`install_directory`*`\VMware\VMware View\Server\sslgateway\conf\`*`truststorefile.key`*

Suivant

Modifiez des propriétés de configuration de Serveur de connexion View pour activer l'authentification par carte à puce.

Modifier des propriétés de configuration de Serveur de connexion View

Pour activer l'authentification par carte à puce, vous devez modifier les propriétés de configuration de Serveur de connexion View sur votre hôte de Serveur de connexion View ou du Serveur de sécurité.

Prérequis

Ajoutez le certificat racine pour tous les utilisateurs approuvés à un fichier du magasin d'approbations du serveur.

Procédure

1 Créez ou modifiez le fichier `locked.properties` dans le dossier de configuration de la passerelle SSL sur l'hôte de Serveur de connexion View ou du Serveur de sécurité.

Par exemple : *`install_directory`*`\VMware\VMware View\Server\sslgateway\conf\locked.properties`

2 Ajoutez les propriétés `trustKeyfile`, `trustStoretype` et `useCertAuth` au fichier `locked.properties`.

a Définissez `trustKeyfile` sur le nom de votre fichier du magasin d'approbations.

b Définissez `trustStoretype` sur **`JKS`**.

c Définissez `useCertAuth` sur **`true`** pour activer l'authentification par certificat.

3 Redémarrez le service Serveur de connexion View ou le service du Serveur de sécurité pour que vos modifications prennent effet.

Exemple : Fichier locked.properties

Le fichier spécifie que le certificat racine de tous les utilisateurs approuvés est situé dans le fichier `lonqa.key`, définit le type de magasin d'approbations sur JKS et active l'authentification par certificat.

```
trustKeyfile=lonqa.key
trustStoretype=JKS
useCertAuth=true
```

Suivant

Si vous avez configuré l'authentification par carte à puce pour une instance de Serveur de connexion View, configurez les paramètres d'authentification par carte à puce dans View Administrator. Vous n'avez pas à configurer des paramètres d'authentification par carte à puce pour un Serveur de sécurité. Les paramètres configurés dans une instance de Serveur de connexion View sont également appliqués à un Serveur de sécurité couplé.

Configurer des paramètres de carte à puce dans View Administrator

Vous pouvez utiliser View Administrator pour spécifier des paramètres afin de s'adapter à différents scénarios d'authentification par carte à puce.

Lorsque vous définissez ces paramètres dans une instance de Serveur de connexion View, les paramètres sont également appliqués aux Serveurs de sécurité couplés.

Prérequis

- Modifiez les propriétés de configuration de Serveur de connexion View sur votre hôte de Serveur de connexion View.
- Vérifiez que les clients View Client établissent des connexions HTTPS directement à l'hôte de Serveur de connexion View ou du Serveur de sécurité. L'authentification par carte à puce n'est pas prise en charge si vous déchargez SSL vers un périphérique intermédiaire qui établit des connexions HTTP à l'hôte Serveur de connexion View ou du Serveur de sécurité.

Procédure

1 Dans View Administrator, cliquez sur **[View Configuration (Configuration de View)] > [Servers (Serveurs)]** .

2 Sélectionnez l'instance de Serveur de connexion View et cliquez sur **[Edit (Modifier)]** .

3 Sous l'onglet **[Authentication (Authentification)]** , sélectionnez une option de configuration dans le menu déroulant **[Smart card authentication (Authentification par carte à puce)]** .

Option	Action
Not Allowed (Non autorisée)	L'authentification par carte à puce est désactivée sur l'instance de Serveur de connexion View.
Optional (Facultative)	Les utilisateurs peuvent utiliser l'authentification par carte à puce ou l'authentification par mot de passe pour se connecter à l'instance de Serveur de connexion View. Si l'authentification par carte à puce échoue, l'utilisateur doit fournir un mot de passe.
Requis	Les utilisateurs doivent utiliser l'authentification par carte à puce lorsqu'ils se connectent à l'instance de Serveur de connexion View. Lorsque l'authentification par carte à puce est requise, l'authentification échoue pour les utilisateurs qui cochent la case **[Log in as current user (Se connecter en tant qu'utilisateur actuel)]** lorsqu'ils se connectent à l'instance de Serveur de connexion View. Ces utilisateurs doivent se réauthentifier avec leur carte à puce et leur code PIN lorsqu'ils ouvrent une session sur Serveur de connexion View. **Remarque** L'authentification par carte à puce ne remplace que l'authentification par mot de passe de Windows. Si SecurID est activé, les utilisateurs doivent s'authentifier en utilisant à la fois SecurID et l'authentification par carte à puce.

4 Configurez la règle de retrait de carte à puce.

Vous ne pouvez pas configurer la règle de retrait de carte à puce lorsque l'authentification par carte à puce est définie sur **[Not Allowed (Non autorisée)]** .

Option	Action
Déconnecter des utilisateurs de Serveur de connexion View lorsqu'ils retirent leurs cartes à puce	Cochez la case **[Disconnect user sessions on smart card removal (Déconnecter les sessions utilisateur lors du retrait de la carte à puce)]** .
Laisser les utilisateurs connectés à Serveur de connexion View lorsqu'ils retirent leurs cartes à puce et les laisser démarrer de nouvelles sessions de poste de travail sans se réauthentifier	Décochez la case **[Disconnect user sessions on smart card removal (Déconnecter les sessions utilisateur lors du retrait de la carte à puce)]** .

La règle de retrait de la carte à puce ne s'applique pas aux utilisateurs qui se connectent à l'instance de Serveur de connexion View lorsque la case **[Log in as current user (Se connecter en tant qu'utilisateur actuel)]** est cochée, même s'ils ouvrent une session sur leur système client avec une carte à puce.

Pour les utilisateurs qui exécutent des postes de travail View localement sur leurs systèmes client, si la règle est définie sur Disconnect user sessions on smart card removal (Déconnecter les sessions utilisateur lors du retrait de la carte à puce), le Système d'exploitation client dans le poste de travail View est verrouillé lorsque les utilisateurs retirent leur carte à puce. La fenêtre de View Client reste ouverte, et les utilisateurs peuvent sélectionner **[Options]** > **[Send Ctrl-Alt-Delete (Envoyer Ctrl-Alt-Suppr)]** pour se réauthentifier.

5 Cliquez sur **[OK]** .

6 Redémarrez le service Serveur de connexion View.

Vous devez redémarrer le service Serveur de connexion View pour que les modifications des paramètres de carte à puce prennent effet, avec une exception. Vous pouvez affecter au paramètre **[Smart card authentication (Authentification par carte à puce)]** la valeur **[Optional (Facultatif)]** ou **[Required (Requise)]** sans avoir à redémarrer le service Serveur de connexion View.

Les utilisateurs dont la session est actuellement ouverte ne sont pas affectés par les modifications apportées aux paramètres de carte à puce.

Suivant

Préparez Active Directory pour l'authentification par carte à puce, si nécessaire. Reportez-vous à la section « Préparer Active Directory pour l'authentification par carte à puce », page 185.

Vérifiez votre configuration d'authentification par carte à puce. Reportez-vous à la section « Vérifier votre configuration de l'authentification par carte à puce », page 188.

Préparer Active Directory pour l'authentification par carte à puce

Vous devrez peut-être effectuer certaines tâches dans Active Directory lors de l'implémentation de l'authentification par carte à puce.

- Ajouter des UPN pour des utilisateurs de carte à puce page 186

  Comme les ouvertures de session par carte à puce reposent sur des noms d'utilisateur principaux (UPN), les comptes d'utilisateurs Active Directory qui utilisent des cartes à puce pour s'authentifier dans View doivent avoir un UPN valide.

- Ajouter le certificat racine au magasin Enterprise NTAuth page 187

  Si vous utilisez une autorité de certification pour émettre des certificats d'ouverture de session par carte à puce ou de contrôleur de domaine, vous devez ajouter le certificat racine au magasin Enterprise NTAuth dans Active Directory. Vous n'avez pas à effectuer cette procédure si le contrôleur de domaine Windows agit en tant qu'autorité de certification racine.

- Ajouter le certificat racine à des autorités de certification racine de confiance page 187

  Si vous utilisez une autorité de certification pour émettre des certificats d'ouverture de session par carte à puce ou de contrôleur de domaine, vous devez ajouter le certificat racine à la stratégie de groupe Trusted Root Certification Authorities (Autorités de certification racine de confiance) dans Active Directory. Vous n'avez pas à effectuer cette procédure si le contrôleur de domaine Windows agit en tant qu'autorité de certification racine.

- Ajouter un certificat intermédiaire à des autorités de certification intermédiaires page 188

  Si vous utilisez une autorité de certification intermédiaire pour émettre des certificats d'ouverture de session par carte à puce ou de contrôleur de domaine, vous devez ajouter le certificat intermédiaire à la stratégie de groupe Intermediate Certification Authorities (Autorités de certification intermédiaires) dans Active Directory.

Ajouter des UPN pour des utilisateurs de carte à puce

Comme les ouvertures de session par carte à puce reposent sur des noms d'utilisateur principaux (UPN), les comptes d'utilisateurs Active Directory qui utilisent des cartes à puce pour s'authentifier dans View doivent avoir un UPN valide.

Si le domaine sur lequel réside un utilisateur de carte à puce est différent du domaine à partir duquel est émis votre certificat racine, vous devez définir l'UPN de l'utilisateur sur l'autre nom de l'objet (SAN) contenu dans le certificat racine de l'autorité de certification approuvée. Si votre certificat racine est émis à partir d'un serveur dans le domaine actuel de l'utilisateur de carte à puce, vous n'avez pas à modifier l'UPN de l'utilisateur.

Remarque Vous devrez peut-être définir l'UPN pour les comptes Active Directory intégrés, même si le certificat est émis à partir du même domaine. Aucun UPN n'est défini par défaut pour les comptes intégrés, y compris Administrateur.

Prérequis

- Obtenez le SAN contenu dans le certificat racine de l'autorité de certification approuvée en affichant les propriétés du certificat.
- Si l'utilitaire Éditeur ADSI n'est pas présent sur votre serveur Active Directory, téléchargez et installez les outils de support Windows appropriés sur le site Web Microsoft.

Procédure

1. Sur votre serveur Active Directory, démarrez l'utilitaire Éditeur ADSI.
2. Dans le volet de gauche, développez le domaine dans lequel se trouve l'utilisateur et double-cliquez sur `CN=Users`.
3. Dans le volet de droite, cliquez avec le bouton droit sur l'utilisateur et cliquez sur **[Properties (Propriétés)]** .
4. Double-cliquez sur l'attribut `userPrincipalName` et saisissez la valeur SAN du certificat de l'autorité de certification approuvée.
5. Cliquez sur **[OK]** pour enregistrer le paramètre d'attribut.

Ajouter le certificat racine au magasin Enterprise NTAuth

Si vous utilisez une autorité de certification pour émettre des certificats d'ouverture de session par carte à puce ou de contrôleur de domaine, vous devez ajouter le certificat racine au magasin Enterprise NTAuth dans Active Directory. Vous n'avez pas à effectuer cette procédure si le contrôleur de domaine Windows agit en tant qu'autorité de certification racine.

Procédure

- Sur votre serveur Active Directory, utilisez la commande `certutil` pour publier le certificat dans le magasin Enterprise NTAuth.

  Par exemple : **`certutil –dspublish –f`** ***`path_to_root_CA_cert`*** **`NTAuthCA`**

L'autorité de certification est désormais approuvée pour émettre des certificats de ce type.

Ajouter le certificat racine à des autorités de certification racine de confiance

Si vous utilisez une autorité de certification pour émettre des certificats d'ouverture de session par carte à puce ou de contrôleur de domaine, vous devez ajouter le certificat racine à la stratégie de groupe Trusted Root Certification Authorities (Autorités de certification racine de confiance) dans Active Directory. Vous n'avez pas à effectuer cette procédure si le contrôleur de domaine Windows agit en tant qu'autorité de certification racine.

Procédure

1 Sur le serveur Active Directory, naviguez vers le plug-in de gestion de stratégie de groupe.

Version d'AD	Chemin de navigation
Windows 2003	a Sélectionnez **[Démarrer] > [Tous les programmes] > [Outils d'administration] > [Utilisateurs et ordinateurs Active Directory]** . b Cliquez avec le bouton droit sur votre domaine et cliquez sur **[Propriétés]** . c Sur l'onglet **[Stratégie de groupe]** , cliquez sur **[Ouvrir]** pour ouvrir le plug-in de Gestion de stratégie de groupe. d Cliquez avec le bouton droit sur **[Stratégie de domaine par défaut]** et cliquez sur **[Modifier]** .
Windows 2008	a Sélectionnez **[Démarrer] > [Outils d'administration] > [Gestion de stratégie de groupe]** . b Développez votre domaine, cliquez avec le bouton droit sur **[Stratégie de domaine par défaut]** et cliquez sur **[Modifier]** .

2 Développez la section **[Computer Configuration (Configuration ordinateur)]** et ouvrez le dossier **[Windows Settings (Paramètres Windows)\Security Settings (Paramètres de sécurité)\Public Key (Clé publique)]** .

3 Cliquez avec le bouton droit sur **[Trusted Root Certification Authorities (Autorités de certification racine de confiance)]** et sélectionnez **[Import (Importer)]** .

4 Suivez les invites de l'assistant pour importer le certificat racine (par exemple, `rootCA.cer`) et cliquez sur **[OK]** .

5 Fermez la fenêtre Group Policy (Stratégie de groupe).

Tous les systèmes du domaine contiennent maintenant une copie du certificat racine dans leur magasin racine approuvé.

Suivant

Si une autorité de certification intermédiaire émet vos certificats d'ouverture de session par carte à puce ou de contrôleur de domaine, ajoutez le certificat intermédiaire à la stratégie de groupe Intermediate Certification Authorities (Autorités de certification intermédiaires) dans Active Directory. Reportez-vous à la section « Ajouter un certificat intermédiaire à des autorités de certification intermédiaires », page 188.

Ajouter un certificat intermédiaire à des autorités de certification intermédiaires

Si vous utilisez une autorité de certification intermédiaire pour émettre des certificats d'ouverture de session par carte à puce ou de contrôleur de domaine, vous devez ajouter le certificat intermédiaire à la stratégie de groupe Intermediate Certification Authorities (Autorités de certification intermédiaires) dans Active Directory.

Procédure

1 Sur le serveur Active Directory, naviguez vers le plug-in de gestion de stratégie de groupe.

Version d'AD	Chemin de navigation
Windows 2003	a Sélectionnez **[Démarrer] > [Tous les programmes] > [Outils d'administration] > [Utilisateurs et ordinateurs Active Directory]** . b Cliquez avec le bouton droit sur votre domaine et cliquez sur **[Propriétés]** . c Sur l'onglet **[Stratégie de groupe]** , cliquez sur **[Ouvrir]** pour ouvrir le plug-in de Gestion de stratégie de groupe. d Cliquez avec le bouton droit sur **[Stratégie de domaine par défaut]** et cliquez sur **[Modifier]** .
Windows 2008	a Sélectionnez **[Démarrer] > [Outils d'administration] > [Gestion de stratégie de groupe]** . b Développez votre domaine, cliquez avec le bouton droit sur **[Stratégie de domaine par défaut]** et cliquez sur **[Modifier]** .

2 Développez la section **[Computer Configuration (Configuration ordinateur)]** et ouvrez la stratégie de **[Windows Settings\Security Settings\Public Key (Paramètres Windows\Paramètres de sécurité\Clé publique)]** .

3 Cliquez avec le bouton droit sur **[Intermediate Certification Authorities (Autorités de certification intermédiaires)]** et sélectionnez **[Import (Importer)]** .

4 Suivez les invites de l'assistant pour importer le certificat intermédiaire (par exemple, `intermediateCA.cer`) et cliquez sur **[OK]** .

5 Fermez la fenêtre Groupe Policy (Stratégie de groupe).

Tous les systèmes du domaine contiennent maintenant une copie du certificat intermédiaire dans leur magasin d'autorité de certification intermédiaire approuvé.

Vérifier votre configuration de l'authentification par carte à puce

Après avoir configuré l'authentification par carte à puce pour la première fois, ou quand l'authentification par carte à puce ne fonctionne pas correctement, vous devez vérifier votre configuration de l'authentification par carte à puce.

Procédure

- Vérifiez que chaque système client comporte View Client, un intergiciel de carte à puce, une carte à puce avec un certificat valide et un lecteur de carte à puce.

  Pour plus d'informations sur la configuration logicielle et matérielle des cartes à puce, consultez la documentation de votre fournisseur de carte à puce.

- Sur chaque système client, sélectionnez **[Start (Démarrer)] > [Settings (Paramètres)] > [Control Panel (Panneau de configuration)] > [Internet Options (Options Internet)] > [Content (Contenu)] > [Certificates (Certificats)] > [Personal (Personnel)]** pour vérifier que des certificats sont disponibles pour l'authentification par carte à puce.

  Lorsqu'un utilisateur insère une carte à puce dans le lecteur de carte à puce, Windows copie les certificats de la carte à puce sur l'ordinateur de l'utilisateur pour que View Client puisse les utiliser.

- Dans le fichier `locked.properties` sur l'hôte de View Connection Server ou du serveur de sécurité, vérifiez que la propriété `useCertAuth` est définie sur **`true`** et qu'elle est bien orthographiée.

  Le fichier `locked.properties` est situé dans *`install_directory`*`\VMware\VMware View\Server\sslgateway\conf`. La propriété `useCertAuth` est souvent mal orthographiée ainsi : `userCertAuth`.

- Si vous avez configuré l'authentification par carte à puce sur une instance de View Connection Server, vérifiez le paramètre d'authentification par carte à puce dans View Administrator.

  a Sélectionnez **[View Configuration (Configuration de View)] > [Servers (Serveurs)]** , sélectionnez l'instance de View Connection Server et cliquez sur **[Edit (Modifier)]** .

  b Sous l'onglet **[Authentication (Authentification)]** , vérifiez que **[Smart card authentication (Authentification par carte à puce)]** est défini sur **[Optional (Facultative)]** ou **[Required (Requise)]** .

  Vous devez redémarrer le service View Connection Server pour que les modifications des paramètres de carte à puce prennent effet.

- Si le domaine sur lequel réside un utilisateur de carte à puce est différent du domaine à partir duquel est émis votre certificat racine, vérifiez que le nom d'utilisateur principal (UPN) de l'utilisateur est défini sur l'autre nom de l'objet (SAN) contenu dans le certificat racine de l'autorité de certification approuvée.

  a Recherchez le SAN contenu dans le certificat racine de l'autorité de certification approuvée en affichant les propriétés du certificat.

  b Sur votre serveur Active Directory, sélectionnez **[Start (Démarrer)] > [Administrative Tools (Outils d'administration)] > [Active Directory Users and Computers (Utilisateurs et ordinateurs Active Directory)]** .

  c Cliquez avec le bouton droit sur le dossier **[Users (Utilisateurs)]** et sélectionnez **[Properties (Propriétés)]** .

  L'UPN apparaît dans les zones de texte **[User logon name (Nom d'ouverture de session de l'utilisateur)]** sous l'onglet **[Account (Compte)]** .

- Si des utilisateurs de carte à puce utilisent le protocole d'affichage PCoIP pour se connecter à des postes de travail View, vérifiez que la sous-fonction PCoIP Smartcard de View Agent est installée sur des sources de postes de travail. La sous-fonction PCoIP Smartcard permet aux utilisateurs de s'authentifier avec des cartes à puce lorsqu'ils utilisent le protocole d'affichage PCoIP.

  REMARQUE La sous-fonction PCoIP Smartcard n'est pas prise en charge sous Windows Vista.

- Vérifiez que les fichiers journaux dans *`drive`*`:\Documents and Settings\All Users\Application Data\VMware\VDM\logs` sur l'hôte de View Connection Server ou du serveur de sécurité contiennent des messages indiquant que l'authentification par carte à puce est activée.

Utilisation de la vérification de la révocation des certificats de carte à puce

Vous pouvez empêcher les utilisateurs avec des certificats utilisateur révoqués de s'authentifier avec des cartes à puce en configurant la vérification de la révocation des certificats. Les certificats sont souvent révoqués lorsqu'un utilisateur quitte une entreprise, perd une carte à puce ou passe d'un service à un autre.

View prend en charge la vérification de la révocation des certificats avec des listes de révocation de certificats (CRL) et avec le protocole OCSP (Online Certificate Status Protocol). Une CRL est une liste de certificats révoqués publiée par l'autorité de certification qui a émis les certificats. OCSP est un protocole de validation de certificat utilisé pour obtenir l'état de révocation d'un certificat X.509.

Vous pouvez configurer la vérification de la révocation des certificats sur une instance de View Connection Server ou sur un serveur de sécurité. Lorsqu'une instance de View Connection Server est couplée avec un serveur de sécurité, vous configurez la vérification de la révocation des certificats sur le serveur de sécurité. L'autorité de certification doit être accessible depuis l'hôte de View Connection Server ou l'hôte du serveur de sécurité.

Vous pouvez configurer la CRL et OCSP sur la même instance de View Connection Server ou sur le même serveur de sécurité. Lorsque vous configurez les deux types de vérification de la révocation des certificats, View tente d'utiliser d'abord OCSP et revient à la CRL si OCSP échoue. View ne revient pas à OCSP si la CRL échoue.

- Ouvrir une session avec la vérification de la liste de révocation de certificats page 190

  Lorsque vous configurez la vérification de la liste de révocation de certificats, View crée et lit une liste de révocation de certificats pour déterminer l'état de révocation d'un certificat utilisateur.

- Ouvrir une session avec la vérification de la révocation des certificats OCSP page 191

  Lorsque vous configurez la vérification de la révocation des certificats OCSP, View envoie une demande à un répondeur OCSP pour déterminer l'état de révocation d'un certificat utilisateur spécifique. View utilise un certificat de signature OCSP pour vérifier que les réponses qu'il reçoit du répondeur OCSP sont authentiques.

- Configurer la vérification de la liste de révocation de certificats page 191

  Lorsque vous configurez la vérification de la liste de révocation de certificats, View lit une liste de révocation de certificats pour déterminer l'état de révocation d'un certificat utilisateur de carte à puce.

- Configurer la vérification de la révocation des certificats OCSP page 192

  Lorsque vous configurez la vérification de la révocation des certificats OCSP, View envoie une demande de vérification à un répondeur OCSP pour déterminer l'état de révocation d'un certificat de carte à puce.

- Propriétés de la vérification de la révocation des certificats de carte à puce page 192

  Vous définissez des valeurs dans le fichier `locked.properties` pour activer et configurer la vérification de la révocation des certificats de carte à puce.

Ouvrir une session avec la vérification de la liste de révocation de certificats

Lorsque vous configurez la vérification de la liste de révocation de certificats, View crée et lit une liste de révocation de certificats pour déterminer l'état de révocation d'un certificat utilisateur.

Si un certificat est révoqué et que l'authentification par carte à puce est facultative, la boîte de dialogue Enter your user name and password (Entrez votre nom d'utilisateur et votre mot de passe) apparaît et l'utilisateur doit fournir un mot de passe pour s'authentifier. Si l'authentification par carte à puce est requise, l'utilisateur reçoit un message d'erreur et n'est pas autorisé à s'authentifier. Les mêmes événements se produisent si View ne peut pas lire la liste de révocation de certificats.

Ouvrir une session avec la vérification de la révocation des certificats OCSP

Lorsque vous configurez la vérification de la révocation des certificats OCSP, View envoie une demande à un répondeur OCSP pour déterminer l'état de révocation d'un certificat utilisateur spécifique. View utilise un certificat de signature OCSP pour vérifier que les réponses qu'il reçoit du répondeur OCSP sont authentiques.

Si le certificat de l'utilisateur est révoqué et que l'authentification par carte à puce est facultative, la boîte de dialogue Enter your user name and password (Entrez votre nom d'utilisateur et votre mot de passe) apparaît et l'utilisateur doit fournir un mot de passe pour s'authentifier. Si l'authentification par carte à puce est requise, l'utilisateur reçoit un message d'erreur et n'est pas autorisé à s'authentifier.

View revient à la vérification de la liste de révocation de certificats s'il ne reçoit pas de réponse du répondeur OCSP ou si la réponse n'est pas valide.

Configurer la vérification de la liste de révocation de certificats

Lorsque vous configurez la vérification de la liste de révocation de certificats, View lit une liste de révocation de certificats pour déterminer l'état de révocation d'un certificat utilisateur de carte à puce.

Prérequis

Familiarisez-vous avec les propriétés du fichier `locked.properties` pour la vérification de la liste de révocation de certificats. Reportez-vous à la section « Propriétés de la vérification de la révocation des certificats de carte à puce », page 192.

Procédure

1 Créez ou modifiez le fichier `locked.properties` dans le dossier de configuration de la passerelle SSL sur l'hôte de View Connection Server ou du serveur de sécurité.

Par exemple : *`install_directory`*`\VMware\VMware View\Server\sslgateway\conf\locked.properties`

2 Ajoutez les propriétés `enableRevocationChecking` et `crlLocation` au fichier `locked.properties`.

a Définissez `enableRevocationChecking` sur **`true`** pour activer la vérification de la révocation des certificats de carte à puce.

b Définissez `crlLocation` sur l'emplacement de la liste de révocation de certificats. La valeur peut être une URL ou un chemin d'accès au fichier.

3 Redémarrez le service Serveur de connexion View ou le service du Serveur de sécurité pour que vos modifications prennent effet.

Exemple : Fichier locked.properties

Le fichier active l'authentification par carte à puce et la vérification de la révocation des certificats de carte à puce, configure la vérification de la liste de révocation de certificats et spécifie une URL pour l'emplacement de la liste de révocation de certificats.

```
trustKeyfile=lonqa.key
trustStoretype=JKS
useCertAuth=true
enableRevocationChecking=true
crlLocation=http://root.ocsp.net/certEnroll/ocsp-ROOT_CA.crl
```

Configurer la vérification de la révocation des certificats OCSP

Lorsque vous configurez la vérification de la révocation des certificats OCSP, View envoie une demande de vérification à un répondeur OCSP pour déterminer l'état de révocation d'un certificat de carte à puce.

Prérequis

Familiarisez-vous avec les propriétés du fichier `locked.properties` pour la vérification de la révocation des certificats OCSP. Reportez-vous à la section « Propriétés de la vérification de la révocation des certificats de carte à puce », page 192.

Procédure

1 Créez ou modifiez le fichier `locked.properties` dans le dossier de configuration de la passerelle SSL sur l'hôte de View Connection Server ou du serveur de sécurité.

Par exemple : *`install_directory`*`\VMware\VMware View\Server\sslgateway\conf\locked.properties`

2 Ajoutez les propriétés `enableRevocationChecking`, `enableOCSP`, `ocspURL` et `ocspSigningCert` au fichier `locked.properties`.

a Définissez `enableRevocationChecking` sur **`true`** pour activer la vérification de la révocation des certificats de carte à puce.

b Définissez `enableOCSP` sur **`true`** pour activer la vérification de la révocation des certificats OCSP.

c Définissez `ocspURL` sur l'URL du répondeur OCSP.

d Définissez `ocspSigningCert` sur l'emplacement du fichier contenant le certificat de signature du répondeur OCSP.

3 Redémarrez le service Serveur de connexion View ou le service du Serveur de sécurité pour que vos modifications prennent effet.

Exemple : Fichier locked.properties

Le fichier active l'authentification par carte à puce et la vérification de la révocation des certificats de carte à puce, configure à la fois la vérification de la révocation des certificats CRL et OCSP, spécifie l'emplacement du répondeur OCSP et identifie le fichier contenant le certificat de signature OCSP.

```
trustKeyfile=lonqa.key
trustStoretype=JKS
useCertAuth=true
enableRevocationChecking=true
enableOCSP=true
allowCertCRLs=true
ocspSigningCert=te-ca.signing.cer
ocspURL=http://te-ca.lonqa.int/ocsp
```

Propriétés de la vérification de la révocation des certificats de carte à puce

Vous définissez des valeurs dans le fichier `locked.properties` pour activer et configurer la vérification de la révocation des certificats de carte à puce.

Tableau 7-1 répertorie les propriétés du fichier `locked.properties` concernant la vérification de la révocation des certificats.

Tableau 7-1. Propriétés de la vérification de la révocation des certificats de carte à puce

Propriété	Description
`enableRevocationChecking`	Définissez cette propriété sur **`true`** pour activer la vérification de la révocation des certificats. Lorsque cette propriété est définie sur **`false`**, la vérification de la révocation des certificats est désactivée et toutes les autres propriétés de vérification de la révocation des certificats sont ignorées. La valeur par défaut est **`false`**.
`crlLocation`	Spécifie l'emplacement de la liste de révocation de certificats, qui peut être une URL ou un chemin de fichier. Si vous ne spécifiez pas d'URL, ou si l'URL spécifiée n'est pas valide, View utilise la liste de révocation de certificats sur le certificat utilisateur si `allowCertCRLs` est défini sur **`true`** ou n'est pas spécifié. Si View ne peut pas accéder à une liste de révocation de certificats, la vérification de la liste de révocation de certificats échoue.
`allowCertCRLs`	Lorsque cette propriété est définie sur **`true`**, View extrait une liste de révocation de certificats du certificat utilisateur. La valeur par défaut est **`true`**.
`enableOCSP`	Définissez cette propriété sur **`true`** pour activer la vérification de la révocation des certificats OCSP. La valeur par défaut est **`false`**.
`ocspURL`	Spécifie l'URL d'un répondeur OCSP.
`ocspResponderCert`	Spécifie le fichier contenant le certificat de signature du répondeur OCSP. View utilise ce certificat pour vérifier que les réponses du répondeur OCSP sont authentiques.
`ocspSendNonce`	Lorsque cette propriété est définie sur **`true`**, une valeur unique est envoyée avec des demandes OCSP pour empêcher les réponses répétées. La valeur par défaut est **`false`**.
`ocspCRLFailover`	Lorsque cette propriété est définie sur **`true`**, View utilise la vérification de la liste de révocation de certificats si la vérification de la révocation des certificats OCSP échoue. La valeur par défaut est **`true`**.

Utilisation de l'authentification à deux facteurs

Vous pouvez configurer une instance de Serveur de connexion View pour que les utilisateurs soient obligés d'utiliser l'authentification RSA SecurID ou RADIUS (Remote Authentication Dial-In User Service).

Avec Horizon View 5.1 et versions supérieures, la prise en charge de RADIUS a été ajoutée à la fonction d'authentification à deux facteurs incluse avec Horizon View :

- La prise en charge de RADIUS offre une large gamme d'autres options d'authentification à deux facteurs basée sur des jetons.
- Horizon View fournit maintenant une interface d'extension standard ouverte pour permettre aux fournisseurs de solutions tiers d'intégrer des extensions d'authentification avancées dans Horizon View.

Comme les solutions d'authentification à deux facteurs, telles que RSA SecurID et RADIUS, fonctionnent avec les gestionnaires d'authentification installés sur des serveurs séparés, vous devez avoir configuré ces serveurs et les rendre accessibles à l'hôte de Serveur de connexion View. Par exemple, si vous utilisez RSA SecurID, le gestionnaire d'authentification utilise RSA Authentication Manager. Si vous disposez de RADIUS, le gestionnaire d'authentification sera un serveur RADIUS.

Pour utiliser l'authentification à deux facteurs, chaque utilisateur doit posséder un jeton, tel qu'un jeton RSA SecurID, qui est enregistré avec son gestionnaire d'authentification. Un jeton d'authentification à deux facteurs est un élément matériel ou logiciel qui génère un code d'authentification à intervalles fixes. Souvent, l'authentification requiert de connaître un code PIN et un code d'authentification.

Si vous possédez plusieurs instances de Serveur de connexion View, vous pouvez configurer l'authentification à deux facteurs sur certaines instances et configurer une méthode d'authentification utilisateur différente sur d'autres. Par exemple, vous pouvez configurer l'authentification à deux facteurs uniquement pour les utilisateurs qui accèdent à des postes de travail View à distance sur Internet.

View est certifié par le programme RSA SecurID Ready et prend en charge l'ensemble des fonctionnalités SecurID, y compris New PIN Mode, Next Token Code Mode, RSA Authentication Manager et l'équilibrage de charge.

- Ouverture de session en utilisant l'authentification à deux facteurs page 194

  Lorsqu'un utilisateur se connecte à une instance de Serveur de connexion View sur laquelle l'authentification RSA SecurID ou RADIUS est activée, une boîte de dialogue d'ouverture de session spéciale apparaît dans View Client.

- Activer l'authentification à deux dans View Administrator page 195

  Vous activez une instance de Serveur de connexion View pour l'authentification RSA SecurID ou RADIUS en modifiant les paramètres de Serveur de connexion View dans View Administrator.

- Résolution du refus d'accès RSA SecurID page 196

  L'accès est refusé lorsque View Client se connecte avec l'authentification RSA SecurID.

- Dépannage du refus d'accès RADIUS page 197

  L'accès est refusé lorsque View Client se connecte avec l'authentification à deux facteurs RADIUS.

Ouverture de session en utilisant l'authentification à deux facteurs

Lorsqu'un utilisateur se connecte à une instance de Serveur de connexion View sur laquelle l'authentification RSA SecurID ou RADIUS est activée, une boîte de dialogue d'ouverture de session spéciale apparaît dans View Client.

Les utilisateurs entrent leur nom d'utilisateur et leur mot de passe d'authentification RSA SecurID ou RADIUS dans une boîte de dialogue d'ouverture de session spéciale. Un mot de passe d'authentification à deux facteurs se compose généralement d'un code PIN suivi d'un code de jeton.

- Si RSA Authentication Manager demande que les utilisateurs saisissent un nouveau code PIN RSA SecurID après la saisie de leur nom d'utilisateur et de leur mot de passe RSA SecurID, une boîte de dialogue de code PIN apparaît. Après avoir défini un nouveau code PIN, les utilisateurs sont invités à attendre le prochain code de jeton avant d'ouvrir une session. Si RSA Authentication Manager est configuré pour utiliser des codes PIN générés par le système, une boîte de dialogue apparaît pour confirmer le code PIN.
- Lors d'une ouverture de session dans View, l'authentification RADIUS fonctionne pratiquement comme RSA SecurID. Si le serveur RADIUS émet un challenge d'accès, View Client affiche une boîte de dialogue semblable à l'invite RSA SecurID pour le code de jeton suivant. Le support actuel des challenges RADIUS est limité à la demande d'entrée de texte. Le texte de challenge du serveur RADIUS ne s'affiche pas. Les formes plus complexes de challenge, telles que le choix multiple ou la sélection d'image, ne sont pas prises en charge.

Lorsqu'un utilisateur entre ses données d'identification dans View Client, le serveur RADIUS peut envoyer un message SMS, un courrier électronique ou un texte en utilisant un autre mécanisme hors bande, au téléphone cellulaire de l'utilisateur avec un code. L'utilisateur peut entrer ce texte et ce code dans View Client pour terminer l'authentification.

- Comme certains fournisseurs RADIUS permettent d'importer les utilisateurs depuis Active Directory, les utilisateurs finals peuvent recevoir un message demandant les données d'identification Active Directory avant le message demandant un nom d'utilisateur et un mot de passe d'authentification RADIUS.

Activer l'authentification à deux dans View Administrator

Vous activez une instance de Serveur de connexion View pour l'authentification RSA SecurID ou RADIUS en modifiant les paramètres de Serveur de connexion View dans View Administrator.

Prérequis

Installez et configurez le logiciel d'authentification à deux facteurs, tel que RSA SecurID ou RADIUS sur un serveur de gestion de l'authentification.

- Pour l'authentification RSA SecurID, exportez le fichier `sdconf.rec` pour l'instance de Serveur de connexion View depuis RSA Authentication Manager. Voir la documentation RSA Authentication Manager.
- Pour l'authentification RADIUS, suivez la documentation de la configuration du fournisseur. Notez le nom d'hôte ou l'adresse IP du serveur RADIUS, le numéro de port sur lequel il écoute l'authentification RADIUS (1812, généralement), le type d'authentification (PAP, CHAP, MS-CHAPv1 ou MS-CHAPv2) et le secret partagé. Vous entrerez ces valeurs dans View Administrator. Vous pouvez entrer des valeurs pour un authentificateur RADIUS principal et un authentificateur secondaire.

Procédure

1. Dans View Administrator, sélectionnez **[View Configuration (Configuration de View)] > [Servers (Serveurs)]** .
2. Dans l'onglet **[Connection Servers (Serveurs de connexion)]** , sélectionnez le serveur et cliquez sur **[Edit (Modifier)]** .
3. Dans l'onglet **[Authentication (Authentification)]** , dans la liste déroulante **[2-factor authentication (Authentification à deux facteurs)]** de la section Advanced Authentication (Authentification avancée), sélectionnez **[RSA SecureID]** ou **[RADIUS.]**
4. Pour forcer la correspondance des noms d'utilisateur RSA SecurID ou RADIUS avec les noms d'utilisateur dans Active Directory, sélectionnez **[Enforce SecurID and Windows user name matching (Appliquer la correspondance des noms d'utilisateur SecurID et Windows)]** ou **[Enforce 2-factor and Windows user name matching (Appliquer la correspondance des noms d'utilisateur à 2 facteurs et Windows)]** .

   Si vous sélectionnez cette option, les utilisateurs doivent utiliser le même nom d'utilisateur RSA SecurID ou RADIUS pour l'authentification Active Directory. Si vous ne sélectionnez pas cette option, les noms peuvent être différents.
5. Pour RSA SecurID, cliquez sur **[Upload File (Télécharger un fichier)]** , saisissez l'emplacement du fichier `sdconf.rec` ou cliquez sur **[Browse (Parcourir)]** pour rechercher le fichier.

6 Pour l'authentification RADIUS, complétez les champs restants :

a Sélectionnez **[Use the same username and password for RADIUS and Windows authentication (Utiliser les mêmes nom d'utilisateur et mode de passe pour l'authentification RADIUS et Windows)]** si l'authentification RADIUS utilise l'authentification Windows qui déclenche une transmission hors bande d'un code de jeton et que ce dernier est utilisé dans une demande d'authentification RADIUS.

Si vous cochez cette case, les utilisateurs n'ont pas à entrer leurs données d'identification Windows après l'authentification RADIUS si cette dernière utilise le nom d'utilisateur et le mot de passe Windows. Les utilisateurs n'ont pas à entrer de nouveau le nom d'utilisateur et le mot de passe Windows après l'authentification RADIUS.

b Dans la zone déroulante **[Authenticator (Authentificateur)]** , sélectionnez **[Create New Authenticator (Créer un authentificateur)]** et complétez la page.

- Affectez à **[Accounting port (Port de gestion de compte)]** la valeur **[0]** si vous ne voulez pas activer la gestion de comptes RADIUS. Définissez un numéro de port différent de zéro uniquement si le serveur RADIUS prend en charge la collecte des données de gestion de comptes. Si le serveur RADIUS ne prend pas en charge les messages de gestion de comptes et que vous définissez un numéro de port différent de zéro, les messages sont envoyés et ignorés et soumis à un nombre de tentatives de renvoi, ce qui retarde l'authentification.

  Les données de gestion de comptes peuvent être utilisées pour facturer les utilisateurs en fonction du temps d'utilisation et des données. Elles peuvent être également utilisées à des fins statistiques et pour la surveillance générale du réseau.

- Si vous définissez une chaîne de préfixe de domaine, la chaîne est placée au début du nom d'utilisateur lorsqu'il est envoyé au serveur RADIUS. Par exemple, si le nom d'utilisateur entré dans View Client est **`jdoe`** et que le préfixe de domaine **`DOMAIN-A\`** est défini, le nom d'utilisateur **`DOMAIN-A\jdoe`** est envoyé au serveur RADIUS. De même, si vous utilisez la chaîne de suffixe de domaine, ou postfixe, **`@mycorp.com`**, le nom d'utilisateur **`jdoe@mycorp.com`** est envoyé au serveur RADIUS.

7 Cliquez sur **[OK]** pour enregistrer vos modifications.

Vous n'avez pas à redémarrer le service Serveur de connexion View. Les fichiers de configuration nécessaires sont distribués automatiquement et les paramètres de configuration sont appliqués immédiatement.

Lorsque les utilisateurs ouvrent View Client et s'authentifient dans Serveur de connexion View, un message d'invite d'authentification à deux facteurs s'affiche. Pour l'authentification RADIUS, la boîte de dialogue d'ouverture de session affiche des invites textuelles qui contiennent l'étiquette de jeton que vous avez définie.

Suivant

Si vous disposez d'un groupe répliqué d'instances de Serveur de connexion View et voulez configurer également l'authentification dans ces instances, vous pouvez réutiliser la configuration d'authentificateur RADIUS.

Résolution du refus d'accès RSA SecurID

L'accès est refusé lorsque View Client se connecte avec l'authentification RSA SecurID.

Problème

Une connexion View Client avec RSA SecurID affiche `Access Denied` et RSA Authentication Manager Log Monitor affiche l'erreur `Node Verification Failed`.

Cause

Le secret nœud de l'hôte RSA Agent doit être réinitialisé.

Solution

1 Dans View Administrator, sélectionnez **[View Configuration (Configuration de View)] > [Servers (Serveurs)]** .

2 Dans View Connection Servers (Serveurs View Connection Server), sélectionnez le serveur View Connection Server et cliquez sur **[Edit (Modifier)]** .

3 Sous l'onglet **[Authentication (Authentification)]** , sélectionnez **[Clear node secret (Effacer le secret nœud)]** .

4 Cliquez sur **[OK]** pour effacer le secret nœud.

5 Sur l'ordinateur exécutant RSA Authentication Manager, sélectionnez **[Start (Démarrer)] > [Programs (Programmes)] > [RSA Security (Sécurité RSA)] > [RSA Authentication Manager Host Mode (Mode hôte de RSA Authentication Manager)]** .

6 Sélectionnez **[Agent Host (Hôte agent)] > [Edit Agent Host (Modifier l'hôte agent)]** .

7 Sélectionnez **[View Connection Server]** dans la liste et décochez la case **[Node Secret Created (Secret nœud créé)]** .

[Node Secret Created (Secret nœud créé)] est sélectionné par défaut chaque fois que vous le modifiez.

8 Cliquez sur **[OK]** .

Dépannage du refus d'accès RADIUS

L'accès est refusé lorsque View Client se connecte avec l'authentification à deux facteurs RADIUS.

Problème

Une connexion View Client qui utilise l'authentification à deux facteurs RADIUS affiche `Access Denied`.

Cause

RADIUS ne reçoit pas de réponse du serveur RADIUS, ce qui provoque l'expiration de View.

Solution

Les erreurs de configuration courantes suivantes génèrent généralement cette situation :

- Le serveur RADIUS n'a pas été configuré pour accepter l'instance de Serveur de connexion View comme client RADIUS. Chaque instance de Serveur de connexion View utilisant RADIUS doit être définie comme client sur le serveur RADIUS. Voir la documentation du produit d'authentification bifactorielle RADIUS.
- Les valeurs secrètes partagées sur l'instance de Serveur de connexion View et le serveur RADIUS ne correspondent pas.

Utilisation de la fonction Se connecter en tant qu'utilisateur actuel disponible avec View Client Windows

Avec View Client pour Windows, lorsque des utilisateurs cochent la case **[Se connecter en tant qu'utilisateur actuel]** , les informations d'identification qu'ils fournissent lors de l'ouverture de session sur le système client sont utilisées pour les authentifier sur l'instance de Serveur de connexion View et sur le poste de travail View. Aucune autre authentification d'utilisateur n'est requise.

Pour prendre en charge cette fonction, les informations d'identification d'utilisateur sont stockées sur l'instance de Serveur de connexion View et sur le système client.

- Sur l'instance de Serveur de connexion View, les informations d'identification d'utilisateur sont chiffrées et stockées dans la session utilisateur avec le nom d'utilisateur, le domaine et l'UPN facultatif. Les informations d'identification sont ajoutées lors de l'authentification et sont supprimées lors de la destruction de l'objet de session. L'objet de session est détruit quand l'utilisateur ferme sa session, quand la session expire ou quand l'authentification échoue. L'objet de session réside dans une mémoire volatile et n'est pas stocké dans View LDAP ou dans un fichier de disque.
- Sur le système client, les informations d'identification d'utilisateur sont chiffrées et stockées dans un tableau dans Authentication Package, qui est un composant de View Client. Les informations d'identification sont ajoutées au tableau quand l'utilisateur ouvre une session et sont supprimées du tableau quand l'utilisateur ferme sa session. Le tableau réside dans la mémoire volatile.

Les administrateurs peuvent utiliser les paramètres de stratégie de groupe View Client pour contrôler la disponibilité de la case **[Se connecter en tant qu'utilisateur actuel]** et pour spécifier sa valeur par défaut. Les administrateurs peuvent également utiliser la stratégie de groupe pour spécifier quelles instances de Serveur de connexion View acceptent l'identité et les informations d'identification de l'utilisateur qui sont transmises lorsque les utilisateurs cochent la case **[Se connecter en tant qu'utilisateur actuel]** dans View Client.

La fonction Se connecter en tant qu'utilisateur actuel a les restrictions et exigences suivantes :

- Lorsque l'authentification par carte à puce est définie sur Requise sur une instance de Serveur de connexion View, l'authentification échoue pour les utilisateurs qui cochent la case **[Se connecter en tant qu'utilisateur actuel]** lorsqu'ils se connectent à l'instance de Serveur de connexion View. Ces utilisateurs doivent se réauthentifier avec leur carte à puce et leur code PIN lorsqu'ils ouvrent une session sur Serveur de connexion View.
- Les utilisateurs ne peuvent pas emprunter un poste de travail pour une utilisation en mode local s'ils ont coché la case **[Se connecter en tant qu'utilisateur actuel]** lors de l'ouverture de leur session.
- L'heure sur le système sur lequel le client ouvre une session et l'heure sur l'hôte de Serveur de connexion View doivent être synchronisées.
- Si les affectations de droit d'usage **[Accéder à cet ordinateur à partir du réseau]** par défaut sont modifiées sur le système client, elles doivent l'être comme indiqué dans l'article 1025691 de la base de connaissances de VMware.
- La machine client doit pouvoir communiquer avec le serveur Active Directory de l'entreprise et ne pas utiliser les informations d'identification mises en cache pour l'authentification. Par exemple, si des utilisateurs ouvrent une session sur leurs machines client depuis l'extérieur du réseau d'entreprise, les informations d'identification mises en cache sont utilisées pour l'authentification. Si l'utilisateur tente de se connecter à un serveur de sécurité ou à une instance de Serveur de connexion View sans d'abord établir une connexion VPN, il est invité à fournir des informations d'identification, et la fonction Se connecter en tant qu'utilisateur actuel ne fonctionne pas.

Autoriser les utilisateurs à enregistrer les données d'identification

Les administrateurs peuvent configurer Serveur de connexion View pour autoriser les périphériques mobiles View Client à enregistrer le nom d'utilisateur, le mot de passe et les informations de domaine d'un utilisateur. Si les utilisateurs décident de faire enregistrer leurs données d'identification, ces dernières sont ajoutées aux champs d'ouverture de session dans View Client lors des connexions suivantes.

Dans les clients View Client Windows, la fonction d'ouverture de session comme utilisateur en cours évite aux utilisateurs d'entrer plusieurs fois leurs données d'identification. Avec View Client pour les périphériques mobiles, tels qu'Android et iPad, vous pouvez configurer une fonction qui permet d'afficher une case à cocher **[Save Password (Enregistrer le mot de passe)]** dans les boîtes de dialogue d'ouverture de session.

Vous définissez un délai d'expiration maximal qui indique le délai de conservation des données d'identification en définissant une valeur dans View LDAP. La limite du délai d'expiration est définie en minutes. Lorsque vous modifiez View LDAP sur une instance de Serveur de connexion View, la modification est propagée à toutes les instances de Serveur de connexion View.

Prérequis

Pour plus d'informations sur l'utilisation de l'utilitaire ADSI Edit sur votre version du système d'exploitation Windows, consultez le site Web Microsoft TechNet.

Procédure

1 Démarrez l'utilitaire ADSI Edit sur votre hôte de Serveur de connexion View.

2 Dans la boîte de dialogue des paramètres de connexion, sélectionnez ou connectez-vous à **[DC=vdi, DC=vmware, DC=int]** .

3 Dans le volet Computer (Ordinateur), sélectionnez ou tapez **`localhost:389`** ou le nom de domaine complet qualifié (FQDN) de l'hôte de Serveur de connexion View suivi du port 389.

   Par exemple : **`localhost:389`** ou **`mycomputer.mydomain.com:389`**

4 Dans l'objet **[CN=Common, OU=Global, OU=Properties]** , définissez l'attribut **[pae-ClientCredentialCacheTimeout]** .

   Lorsque cet attribut n'est pas défini ou qu'il a la valeur **`0`**, la fonction est désactivée. Pour activer cette fonction, vous pouvez définir le nombre de minutes de conservation des données d'identification ou spécifier la valeur -1, ce qui implique qu'aucun délai d'expiration n'est défini.

Dans Serveur de connexion View, le nouveau paramètre est appliqué immédiatement. Vous n'avez pas à redémarrer le service Serveur de connexion View ou l'ordinateur client.

Configuration de règles

8

Vous pouvez configurer des règles pour contrôler le comportement de composants View, de pools de postes de travail et d'utilisateurs de poste de travail. Vous utilisez View Administrator pour définir des règles pour des sessions client et vous utilisez des paramètres de stratégie de groupe Active Directory pour contrôler le comportement de certaines fonctions et composants View.

Ce chapitre aborde les rubriques suivantes :

Définition de règles dans View Administrator

Vous utilisez View Administrator pour configurer des règles pour des sessions client.

Vous pouvez définir ces règles pour affecter des utilisateurs spécifiques, des pools de postes de travail spécifiques ou tous les utilisateurs de sessions client. Les règles qui affectent des utilisateurs et des pools de postes de travail spécifiques sont appelées règles de niveau utilisateur et règles de niveau poste de travail. Les règles qui affectent toutes les sessions et utilisateurs sont appelées règles générales.

Les règles de niveau utilisateur héritent de paramètres provenant des paramètres de règle de pool/poste de travail équivalents. De la même façon, les règles de niveau pool héritent de paramètres provenant des paramètres de règle générale équivalents. Le paramètre de règle de niveau pool est prioritaire par rapport au paramètre de règle générale équivalent. Le paramètre de règle de niveau utilisateur est prioritaire par rapport aux paramètres de règle générale et de niveau pool équivalents.

Les paramètres de règle de niveau inférieur peuvent être plus ou moins restrictifs que les paramètres de niveau supérieur équivalents. Par exemple, si la règle générale spécifiant la durée pendant laquelle un poste de travail peut être emprunté est définie sur 10 minutes et que la règle de niveau pool équivalente est définie sur 5 minutes, vous pouvez définir la règle de niveau utilisateur équivalente sur 30 minutes pour n'importe quel utilisateur dans le pool.

- Configurer des règles pour des pools de postes de travail page 202

  Vous pouvez configurer des règles de niveau poste de travail pour affecter des pools de postes de travail spécifiques. Les paramètres de règle de niveau poste de travail sont prioritaires par rapport à leurs paramètres de règle générale équivalents.

- Configurer des règles pour les utilisateurs de poste de travail page 203

  Vous pouvez configurer des règles de niveau utilisateur pour affecter des utilisateurs spécifiques. Les paramètres de règle de niveau utilisateur sont toujours prioritaires par rapport aux paramètres de règle générale et de niveau poste de travail équivalents.

- Règles de View page 203

  Vous pouvez configurer des règles View pour affecter toutes les sessions client, ou vous pouvez les appliquer pour affecter des postes de travail ou des utilisateurs spécifiques.

- Règles du mode local page 204

  Vous pouvez configurer des règles de mode local pour affecter toutes les sessions client, ou vous pouvez les appliquer à des postes de travail ou des utilisateurs spécifiques.

Configurer des paramètres de règle générale

Vous pouvez configurer des règles générales pour contrôler le comportement de tous les utilisateurs de sessions client.

Prérequis

Familiarisez-vous avec les descriptions de règles. Pour plus d'informations, reportez-vous aux rubriques suivantes :

- « Règles de View », page 203
- « Règles du mode local », page 204

Procédure

1 Dans View Administrator, sélectionnez **[Policies (Règles)]** > **[Global Policies (Règles générales)]** .

   a Pour configurer des règles de session générale, cliquez sur **[Edit policies (Modifier des règles)]** dans le volet **[View Policies (Règles de View)]** .

   b Pour configurer des règles de session locale, cliquez sur **[Edit policies (Modifier des règles)]** dans le volet **[Local Session Policies (Règles de session locale)]** .

2 Cliquez sur **[OK]** pour enregistrer vos modifications.

Configurer des règles pour des pools de postes de travail

Vous pouvez configurer des règles de niveau poste de travail pour affecter des pools de postes de travail spécifiques. Les paramètres de règle de niveau poste de travail sont prioritaires par rapport à leurs paramètres de règle générale équivalents.

Prérequis

Familiarisez-vous avec les descriptions de règles. Pour plus d'informations, reportez-vous aux rubriques suivantes :

- « Règles de View », page 203
- « Règles du mode local », page 204

Procédure

1 Dans View Administrator, sélectionnez **[Inventory (Inventaire)]** > **[Pools]** .

2 Double-cliquez sur l'ID du pool de postes de travail et cliquez sur l'onglet **[Policies (Règles)]** .

L'onglet **[Policies (Règles)]** montre les paramètres de règle actuels. Lorsqu'un paramètre est hérité de la règle générale équivalente, **[Inherit (Hériter)]** apparaît dans la colonne **[Pool Policy (Règle de pool)]** .

3 Pour configurer des règles de session générale pour le pool, cliquez sur **[Edit policies (Modifier des règles)]** dans le volet **[View Policies (Règles de View)]** .

4 Pour configurer des règles de session locale pour le pool, cliquez sur **[Edit policies (Modifier des règles)]** dans le volet **[Local Mode Policies (Règles du mode local)]** .

5 Cliquez sur **[OK]** pour enregistrer vos modifications.

Configurer des règles pour les utilisateurs de poste de travail

Vous pouvez configurer des règles de niveau utilisateur pour affecter des utilisateurs spécifiques. Les paramètres de règle de niveau utilisateur sont toujours prioritaires par rapport aux paramètres de règle générale et de niveau poste de travail équivalents.

Prérequis

Familiarisez-vous avec les descriptions de règles. Reportez-vous à la section « Règles de View », page 203.

Procédure

1 Dans View Administrator, sélectionnez **[Inventory (Inventaire)]** > **[Pools]** .

2 Double-cliquez sur l'ID du pool de postes de travail et cliquez sur l'onglet **[Policies (Règles)]** .

L'onglet **[Policies (Règles)]** montre les paramètres de règle actuels. Lorsqu'un paramètre est hérité de la règle générale équivalente, **[Inherit (Hériter)]** apparaît dans la colonne **[Pool Policy (Règle de pool)]** .

3 Cliquez sur **[User Overrides (Remplacements d'utilisateur)]** et sur **[Add User (Ajouter un utilisateur)]** .

4 Pour rechercher un utilisateur, cliquez sur **[Add (Ajouter)]** , saisissez le nom ou la description de l'utilisateur, puis cliquez sur **[Find (Rechercher)]** .

5 Sélectionnez un ou plusieurs utilisateurs dans la liste, cliquez sur **[OK]** , puis sur **[Next (Suivant)]** .

La boîte de dialogue Add Individual Policy (Ajouter une règle individuelle) apparaît.

6 Configurez des règles de session générales sous l'onglet **[General (Général)]** .

7 Configurez des règles pour des clients en mode local sous l'onglet **[Local]** .

8 Cliquez sur **[Finish (Terminer)]** pour enregistrer vos modifications.

Règles de View

Vous pouvez configurer des règles View pour affecter toutes les sessions client, ou vous pouvez les appliquer pour affecter des postes de travail ou des utilisateurs spécifiques.

Tableau 8-1 décrit chaque paramètre de règle View.

Tableau 8-1. Règles de View

Règle	Description
Multimedia redirection (MMR) (Redirection multimédia (MMR))	Détermine si MMR est activé pour les systèmes client. MMR est un filtre de Microsoft DirectShow qui permet de transférer des données multimédias de codecs spécifiques sur des postes de travail View au système client directement via un socket TCP. Les données sont ensuite directement décodées sur le système client, lorsqu'elles sont lues. La valeur par défaut est **[Allow (Autoriser)]** . Si des systèmes client disposent de ressources insuffisantes pour gérer le décodage multimédia local, passez le paramètre sur **[Deny (Refuser)]** . MMR ne fonctionne pas correctement si le matériel d'affichage vidéo du système client ne prend pas en charge la superposition.
USB Access (Accès USB)	Détermine si des postes de travail peuvent utiliser des périphériques USB connectés au système client. La valeur par défaut est **[Allow (Autoriser)]** . Pour empêcher l'utilisation de périphériques externes pour des raisons de sécurité, passez le paramètre sur **[Deny (Refuser)]** .
Remote mode (Mode distant)	Détermine si des utilisateurs peuvent se connecter et utiliser des postes de travail exécutés sur des instances de vCenter Server. Si défini sur **[Deny (Refuser)]** , les utilisateurs doivent emprunter le poste de travail sur leurs ordinateurs locaux et exécuter le poste de travail uniquement en mode local. Forcer les utilisateurs à exécuter les postes de travail uniquement en mode local réduit les coûts associés aux exigences de CPU, de mémoire et de bande passante réseau pour l'exécution du poste de travail sur un serveur principal. La valeur par défaut est **[Allow (Autoriser)]** .
PCoIP hardware acceleration (Accélération matérielle PCoIP)	Détermine l'activation de l'accélération matérielle du protocole d'affichage PCoIP et spécifie la priorité d'accélération affectée à la session utilisateur PCoIP. Ce paramètre a un effet uniquement si un périphérique d'accélération matérielle PCoIP est présent sur l'ordinateur physique qui héberge le poste de travail. La valeur par défaut est **[Allow (Autoriser)]** avec une priorité **[Medium (Moyenne)]** .

Règles du mode local

Vous pouvez configurer des règles de mode local pour affecter toutes les sessions client, ou vous pouvez les appliquer à des postes de travail ou des utilisateurs spécifiques.

Tableau 8-2 décrit chaque paramètre de règle de mode local.

Tableau 8-2. Règles du mode local

Règle	Description
Local Mode (Mode local)	Détermine si les utilisateurs peuvent emprunter des postes de travail pour une utilisation locale. Détermine également si les utilisateurs peuvent exécuter des postes de travail locaux lorsque ces postes de travail sont empruntés. La valeur par défaut est **[Deny (Refuser)]** . Si vous réglez cette valeur de **[Allow (Autoriser)]** à **[Deny (Refuser)]** lorsqu'un poste de travail est emprunté, l'utilisateur ne peut pas exécuter le poste de travail en mode local, et le poste de travail ne peut pas être utilisé à distance alors qu'il est toujours emprunté.
User-initiated rollback (Restauration initiée par l'utilisateur)	Détermine si les utilisateurs peuvent ignorer un poste de travail local et revenir à la version distante. Quand un utilisateur initie le processus de restauration, le verrou sur le poste de travail distant est retiré et le poste de travail local est ignoré. Si nécessaire, l'utilisateur peut supprimer manuellement le dossier local contenant les données du poste de travail local. La valeur par défaut est **[Allow (Autoriser)]** .

Tableau 8-2. Règles du mode local (suite)

Règle	Description
Max time without server contact (Durée maximum sans contact avec le serveur)	Spécifie la durée en jours pendant laquelle un poste de travail local peut s'exécuter sans contacter View Connection Server pour les mises à jour de règles. Si la limite de durée spécifiée est dépassée, View Client affiche un message d'avertissement à l'utilisateur et interrompt le poste de travail. La valeur par défaut est de **7** jours. Du côté client, cette règle d'expiration est stockée dans un fichier chiffré par une clé intégrée à l'application. Cette clé intégrée empêche les utilisateurs qui ont accès au mot de passe de contourner la règle d'expiration.
Target replication frequency (Fréquence de réplication cible)	Spécifie l'intervalle en jours, heures ou minutes entre le début d'une réplication et le début de la réplication suivante. Une réplication copie les modifications effectuées dans des fichiers de poste de travail local vers le poste de travail distant correspondant ou le disque persistant de View Composer dans le datacenter. La valeur par défaut est le paramètre **[No replication (Aucune réplication)]** . Si vous sélectionnez **[At a specified interval (À un intervalle spécifique)]** , l'intervalle de réplication par défaut est de 12 heures. Vous pouvez interdire les réplications planifiées en sélectionnant **[No replication (Aucune réplication)]** . La règle **[No replication (Aucune réplication)]** n'interdit pas les demandes de réplication explicites. Vous pouvez initier des réplications dans View Administrator, et les utilisateurs peuvent demander des réplications si la règle **[User initiated replication (Réplication initiée par l'utilisateur)]** est définie sur **[Allow (Autoriser)]** . Si une réplication dure plus longtemps que l'intervalle spécifié dans la règle **[Target replication frequency (Fréquence de réplication cible)]** , la prochaine réplication planifiée démarre après la fin de la précédente. La réplication en attente n'annule pas la précédente. Par exemple, la règle **[Target replication frequency (Fréquence de réplication cible)]** doit être définie sur un jour. Une réplication peut commencer à midi le mardi. Si l'ordinateur client est déconnecté du réseau, la réplication peut durer plus de 24 heures. À midi le mercredi, View Client with Local Mode démarre la prochaine demande de réplication. Après la fin de la réplication précédente, View Client with Local Mode prend un snapshot et démarre la réplication en attente.
User deferred replication (Réplication différée par l'utilisateur)	Détermine si les utilisateurs peuvent suspendre des réplications actives. Si vous activez cette règle, un utilisateur peut différer une réplication en cours. La réplication ne reprend pas, et aucune nouvelle réplication ne démarre, jusqu'à la fin de la période de report. La valeur par défaut est **[Deny (Refuser)]** . Lorsque la valeur est définie sur **[Allow (Autoriser)]** , la période de report est de deux heures.
Disks replicated (Disques répliqués)	Détermine quels disques de poste de travail sont répliqués. Cette règle n'affecte que les postes de travail de clone lié View Composer. Pour les postes de travail de machine virtuelle complète, tous les disques sont répliqués. Vous avez les choix de réplication de disque suivants : ■ Disques persistants ■ disques du système d'exploitation ■ Disques du système d'exploitation et persistants Modifier cette règle affecte la réplication de poste de travail après le prochain emprunt. Une modification n'affecte pas les postes de travail qui sont actuellement empruntés. La valeur par défaut est **[Persistent disks (Disques persistants)]** .

Tableau 8-2. Règles du mode local (suite)

Règle	Description
User-initiated check in (Restitution initiée par l'utilisateur)	Détermine si des utilisateurs sont autorisés à restituer des postes de travail exécutés en mode local. La valeur par défaut est **[Allow (Autoriser)]** .
User-initiated replication (Réplication initiée par l'utilisateur)	Détermine si des utilisateurs sont autorisés à initier des réplications depuis leurs postes de travail quand ils sont exécutés en mode local. La valeur par défaut est **[Allow (Autoriser)]** .

Utilisation de stratégies de groupe Active Directory

Vous pouvez utiliser une stratégie de groupe Microsoft Windows pour optimiser et sécuriser des postes de travail View, contrôler le comportement de composants View et configurer l'impression basée sur l'emplacement.

La stratégie de groupe est une fonction des systèmes d'exploitation Microsoft Windows qui fournit une gestion et une configuration centralisées des ordinateurs et des utilisateurs à distance dans un environnement Active Directory.

Les paramètres de stratégie de groupe sont contenus dans des entités appelées GPO. Des GPO sont associés à des objets Active Directory. Vous pouvez appliquer des GPO à des composants View à un niveau domaine pour contrôler diverses zones de l'environnement View. Une fois appliqués, les paramètres de GPO sont stockés dans le Registre Windows local du composant spécifié.

Vous utilisez l'Éditeur d'objets de stratégie de groupe de Microsoft Windows pour gérer des paramètres de stratégie de groupe. L'Éditeur d'objets de stratégie de groupe est un composant logiciel enfichable de Microsoft Management Console (MMC). La MMC fait partie de la Console de gestion des stratégies de groupe (GPMC). Pour plus d'informations sur l'installation et l'utilisation de la GPMC, consultez le site Web Microsoft TechNet.

Création d'une UO pour des postes de travail View

Vous devez créer une unité d'organisation (UO) dans Active Directory spécifiquement pour vos postes de travail View.

Pour empêcher l'application de paramètres de règle de groupe sur d'autres serveurs ou stations de travail Windows dans le même domaine que vos postes de travail, créez un objet de stratégie de groupe (GPO) pour vos stratégies de groupe View et liez-le à l'UO qui contient vos postes de travail View.

Pour plus d'informations sur la création d'UO et de GPO, consultez la documentation à propos de Microsoft Active Directory sur le site Web Microsoft TechNet.

Activation du traitement en boucle pour des postes de travail View

Par défaut, les paramètres de stratégie d'un utilisateur viennent de l'ensemble de GPO appliqués à l'objet utilisateur dans Active Directory. Toutefois, dans l'environnement View, des GPO doivent s'appliquer à des utilisateurs en fonction de l'ordinateur sur lequel ils ouvrent une session.

Lorsque vous activez le traitement en boucle, un ensemble cohérent de règles s'applique à tous les utilisateurs qui ouvrent une session sur un ordinateur particulier, peu importe l'emplacement de ces règles dans Active Directory.

Pour plus d'informations sur l'activation du traitement en boucle, consultez la documentation à propos de Microsoft Active Directory.

Remarque Le traitement en boucle est seulement une des approches existantes pour gérer les GPO dans View. Vous devrez peut-être implémenter une approche différente.

Utilisation de fichiers de modèle d'administration de stratégie de groupe de View

View comporte plusieurs fichiers de modèle d'administration de stratégie de groupe spécifiques à un composant. Vous pouvez optimiser et sécuriser des postes de travail View en ajoutant les paramètres de stratégie dans ces fichiers de modèle d'administration à un nouveau GPO ou à un GPO existant dans Active Directory.

Les fichiers de modèle d'administration de View contiennent des stratégies de groupe Configuration d'ordinateur et Configuration d'utilisateur.

- Les stratégies Configuration d'ordinateur définissent des stratégies qui s'appliquent à tous les postes de travail View, quelle que soit la personne se connectant au poste de travail.
- Les stratégies Configuration d'utilisateur définissent des stratégies qui s'appliquent à tous les utilisateurs, quel que soit le poste de travail View auquel ils se connectent. Les stratégies Configuration d'utilisateur remplacent les stratégies Configuration d'ordinateur équivalentes.

View applique des stratégies au démarrage de poste de travail View et quand les utilisateurs ouvrent une session.

Fichiers de modèle d'administration de View

Les fichiers de modèle d'administration de View sont installés dans le répertoire *install_directory*\VMware\VMware View\Server\extras\GroupPolicyFiles sur votre hôte de View Connection Server.

Tableau 8-3. Fichiers de modèle d'administration de View

Nom du modèle	Fichier de modèle	Description
Configuration de VMware View Agent	vdm_agent.adm	Contient des paramètres de stratégie liés aux composants d'authentification et d'environnement de View Agent.
Configuration de VMware View Client	vdm_client.adm	Contient des paramètres de stratégie liés à la configuration de View Client. Les clients qui se connectent depuis l'extérieur du domaine d'hôte de View Connection Server ne sont pas affectés par des règles appliquées à View Client.
Configuration de VMware View Server	vdm_server.adm	Contient des paramètres de stratégie liés à View Connection Server.
Configuration commune de VMware View	vdm_common.adm	Contient des paramètres de stratégie communs à tous les composants View.
Variables de session PCoIP de VMware View	pcoip.adm	Contient des paramètres de stratégie liés au protocole d'affichage PCoIP.
Configuration de VMware View Persona Management	ViewPM.adm	Contient des paramètres de stratégie liés à View Persona Management. Reportez-vous à la section « Paramètres de stratégie de groupe Gestion de persona View », page 279.

Paramètres de modèle d'administration pour la configuration de View Agent

Le fichier de modèle d'administration pour la configuration de View Agent (`vdm_agent.adm`) contient des paramètres de stratégie liés aux composants d'authentification et d'environnement de View Agent.

Tableau 8-4 décrit les paramètres de règle dans le fichier de modèle d'administration pour la configuration de View Agent différents de ceux utilisés avec des périphériques USB. Le modèle contient les paramètres de Configuration d'ordinateur et de Configuration d'utilisateur. Le paramètre de Configuration d'utilisateur remplace le paramètre de Configuration d'ordinateur équivalent.

Tableau 8-4. Paramètres de modèle pour la configuration de View Agent

Paramètre	Ordinateur	Utilisateur	Propriétés
`AllowDirectRDP`	X		Détermine si les clients non View peuvent se connecter directement à des postes de travail View avec RDP. Lorsque ce paramètre est désactivé, View Agent n'autorise que les connexions gérées par View via View Client. Lorsque vous vous connectez à un poste de travail virtuel à partir de View Client pour Mac OS X, ne désactivez pas le paramètre `AllowDirectRDP`. Si ce paramètre est désactivé, la connexion échoue avec une erreur `Accès refusé`. Par défaut, lorsqu'un utilisateur a ouvert une session sur un poste de travail View, vous pouvez utiliser RDP pour vous connecter à la machine virtuelle de poste de travail depuis l'extérieur de View. La connexion RDP met fin à la session du poste de travail View et les données et paramètres non enregistrés de l'utilisateur View peuvent être perdus. L'utilisateur View ne peut pas ouvrir de session sur le poste de travail tant que la connexion RDP externe n'est pas fermée. Pour éviter cette situation, désactivez le paramètre `AllowDirectRDP`. Ce paramètre est activé par défaut.
`AllowSingleSignon`	X		Détermine si une authentification unique (SSO) est utilisée pour connecter des utilisateurs à des postes de travail View. Lorsque ce paramètre est activé, les utilisateurs doivent uniquement saisir leurs informations d'identification lors de la connexion à View Client. Lorsqu'il est désactivé, les utilisateurs doivent s'authentifier de nouveau lorsque la connexion à distance est effectuée. Ce paramètre est activé par défaut.
`CommandsToRunOnConnect`	X		Spécifie une liste de commandes ou de scripts de commande à exécuter lorsqu'une session est connectée pour la première fois. Reportez-vous à la section « Exécution de commandes sur des postes de travail View », page 213 pour plus d'informations.
`CommandsToRunOnReconnect`	X		Spécifie une liste de commandes ou de scripts de commande à exécuter lorsqu'une session est reconnectée après une déconnexion. Reportez-vous à la section « Exécution de commandes sur des postes de travail View », page 213 pour plus d'informations.

Tableau 8-4. Paramètres de modèle pour la configuration de View Agent (suite)

Paramètre	Ordinateur	Utilisateur	Propriétés
`Se connecter avec un nom DNS`	X		Détermine si Serveur de connexion View utilise le nom DNS à la place de l'adresse IP de l'hôte lors de la connexion. Ce paramètre est généralement activé dans une situation NAT ou de pare-feu dans laquelle View Client ou Serveur de connexion View ne peut pas utiliser directement l'adresse IP du poste de travail. Ce paramètre est désactivé par défaut.
`ConnectionTicketTimeout`	X		Spécifie la durée en secondes pendant laquelle le ticket de connexion View est valide. Les clients View utilisent un ticket de connexion pour la vérification et l'authentification unique lors de la connexion à View Agent. Pour des raisons de sécurité, un ticket de connexion est valide pendant une durée limitée. Lorsqu'un utilisateur se connecte à un poste de travail View, l'authentification doit avoir lieu pendant le délai d'expiration du ticket de connexion sinon la session expire. Si ce paramètre n'est pas configuré, le délai d'expiration par défaut est de 900 secondes.
`CredentialFilterExceptions`	X		Spécifie les fichiers exécutables qui ne sont pas autorisés à charger l'agent CredentialFilter. Les noms de fichier ne doivent pas contenir de chemin d'accès ou de suffixe. Utilisez un point-virgule pour séparer plusieurs noms de fichier.
`Désactiver la synchronisation du fuseau horaire`	X	X	Détermine si le fuseau horaire du poste de travail View est synchronisé avec celui du client connecté. Un paramètre activé ne s'applique que si le paramètre `Désactiver le transfert de fuseau horaire` de la règle de configuration de View Client n'est pas réglé sur désactivé. Ce paramètre est désactivé par défaut.
`Activer l'accélération multimédia`	X		Détermine si la redirection multimédia (MMR) est activée sur le poste de travail View. MMR est un filtre de Microsoft DirectShow qui permet de transférer des données multimédia de codecs spécifiques sur le système distant au client directement via un socket TCP. Les données sont ensuite décodées directement sur le client, lorsqu'elles sont lues. Vous pouvez désactiver MMR si le client ne dispose pas de ressources suffisantes pour gérer le décodage multimédia local. MMR ne fonctionne pas correctement si le matériel d'affichage vidéo de View Client ne prend pas en charge la superposition. La règle MMR ne s'applique pas aux sessions de poste de travail local. Ce paramètre est activé par défaut.
`Forcer MMR à utiliser la superposition logicielle`	X		Détermine si la fonction de redirection multimédia (MMR) utilise une superposition logicielle à la place d'une superposition matérielle. MMR utilise le matériel d'affichage vidéo avec la prise en charge de la superposition pour de meilleures performances. Comme les superpositions matérielles n'existent en général que sur l'écran principal d'un système à plusieurs écrans, la vidéo n'est pas affichée quand elle est glissée de l'écran principal vers un écran secondaire. L'activation de ce paramètre force MMR à utiliser une superposition matérielle sur tous les écrans. Ce paramètre est désactivé par défaut.

Tableau 8-4. Paramètres de modèle pour la configuration de View Agent (suite)

Paramètre	Ordinateur	Utilisateur	Propriétés
`ShowDiskActivityIcon`	X		Ce paramètre n'est pas pris en charge dans cette version.
`Basculer le contrôle des paramètres d'affichage`	X		Détermine si l'onglet **[Paramètres]** du panneau de configuration **[Affichage]** est désactivé lorsqu'une session client utilise le protocole d'affichage PCoIP. Ce paramètre est activé par défaut.

Paramètres USB pour View Agent

Vous pouvez définir des paramètres de règle USB pour View Agent et View Client pour Windows. Lors de la connexion, View Client télécharge les paramètres de règle USB depuis View Agent et les utilise avec les paramètres de règle USB de View Client afin de décider les périphériques qu'il va rendre disponible pour la redirection depuis l'ordinateur client.

Les paramètres s'appliquent au niveau de l'ordinateur. De préférence, View Agent lit les paramètres depuis le GPO au niveau de l'ordinateur. Sinon, il les lit depuis le registre dans `HKLM\Software\Policies\VMware, Inc.\VMware VDM\Agent\USB`

Tableau 8-5 décrit chaque paramètre de règle pour fractionner des périphériques USB composites dans le fichier de modèle d'administration pour la configuration de View Agent. View Agent n'applique pas ces paramètres. View Agent transmet les paramètres à View Client pour interprétation et application selon que vous spécifiez le modificateur de fusion (`m`) ou de remplacement (`o`). View Client utilise les paramètres pour décider de fractionner des périphériques USB composites en périphériques composants, et d'exclure les périphériques composants de la redirection. Pour voir une description de la façon dont View applique les règles pour le fractionnement de périphériques USB composites, reportez-vous à la section « Configuration de paramètres de règle de fractionnement de périphérique pour des périphériques USB composites », page 228.

Tableau 8-5. Modèle pour la configuration de View Agent : paramètres de fractionnement de périphérique

Paramètre	Propriétés
`Autoriser le fractionnement automatique de périphérique`	Autorise le fractionnement automatique de périphériques USB composites. La valeur par défaut n'est pas définie.
`Exclude Vid/Pid Device From Split`	Exclut un périphérique USB composite spécifié par des ID de fournisseur et de produit du fractionnement. Le format du paramètre est {`m`|`o`}`:vid-`*xxx1*`_pid-`*yyy2*[`;vid-`*xxx2*`_pid-`*yyy2*]... Vous devez spécifier des numéros d'ID au format hexadécimal. Vous pouvez utiliser le caractère générique (`*`) à la place de chiffres dans un ID. Par exemple : **`o:vid-0781_pid-55**`** La valeur par défaut n'est pas définie.
`Split Vid/Pid Device`	Traite les composants d'un périphérique USB composite spécifiés par des ID de fournisseur et de produit en tant que périphériques séparés. Le format du paramètre est {`m`|`o`}`:vid-`*xxxx*`_pid-`*yyyy*`(exintf:`*zz*[`;exintf:`*ww*]) ou {`m`|`o`}`:vid-`*xxxx*`_pid-`*yyyy*`(exintf:`*zz*[`;exintf:`*ww*]) Vous pouvez utiliser le mot-clé **`exintf`** pour exclure des composants de la redirection en spécifiant leur numéro d'interface. Vous devez spécifier les numéros d'ID au format hexadécimal et les numéros d'interface au format décimal en incluant les zéros à gauche. Vous pouvez utiliser le caractère générique (`*`) à la place de chiffres dans un ID. Par exemple : **`o:vid-0781_pid-554c(exintf:01;exintf:02)`** **Remarque** View n'inclut pas automatiquement les composants que vous n'avez pas explicitement exclus. Vous devez spécifier une règle de filtre telle que `Include Vid/Pid Device` pour inclure ces composants. La valeur par défaut n'est pas définie.

Tableau 8-6 décrit chaque paramètre de règle appliquée par un agent pour USB dans le fichier de modèle d'administration pour la configuration de View Agent. View Agent utilise les paramètres pour décider si un périphérique USB peut être transmis à la machine hôte. View Agent transmet également les paramètres à View Client pour interprétation et application selon que vous spécifiez le modificateur de fusion (`m`) ou de remplacement (`o`). View Client utilise les paramètres pour décider si un périphérique USB est disponible pour la redirection. Comme View Agent applique toujours un paramètre de règle appliquée par un agent que vous spécifiez, l'effet peut être la neutralisation de la règle que vous avez définie pour View Client. Pour voir une description de la façon dont View applique les règles pour le filtrage de périphériques USB, reportez-vous à la section « Configuration de paramètres de règle de filtre pour des périphériques USB », page 231.

Tableau 8-6. Modèle pour la configuration de View Agent : paramètres appliqués par un agent

Paramètre	Propriétés
`Exclude All Devices`	Exclut tous les périphériques USB de la transmission. Si ce paramètre est défini sur **`true`**, vous pouvez utiliser d'autres paramètres de règle pour autoriser la transmission de périphériques spécifiques ou de familles de périphériques. Si ce paramètre est défini sur **`false`**, vous pouvez utiliser d'autres paramètres de règle pour empêcher la transmission de périphériques spécifiques ou de familles de périphériques. Si ce paramètre est défini sur **`true`** et transmis à View Client, ce paramètre remplace toujours le paramètre sur View Client. Vous ne pouvez pas utiliser le modificateur de fusion (`m`) ou de remplacement (`o`) avec ce paramètre. La valeur par défaut n'est pas définie, ce qui équivaut à **`false`**.
`Exclude Device Family`	Exclut des familles de périphériques de la transmission. Le format du paramètre est {`m`|`o`}`:`*family_name_1*[`;`*family_name_2*]... Par exemple : **`o:bluetooth;smart-card`** Si vous avez activé le fractionnement automatique de périphérique, View examine la famille de périphériques de chaque interface d'un périphérique USB composite pour décider quelles interfaces doivent être exclues. Si vous avez désactivé le fractionnement automatique de périphérique, View examine la famille de périphérique de l'ensemble du périphérique USB composite. La valeur par défaut n'est pas définie.
`Exclure un périphérique Vid/Pid`	Exclut des périphériques avec des ID de fournisseur et de produit spécifiés de la transmission. Le format du paramètre est {`m`|`o`}`:vid-`*xxx1*`_pid-`*yyy2*[`;vid-`*xxx2*`_pid-`*yyy2*]... Vous devez spécifier des numéros d'ID au format hexadécimal. Vous pouvez utiliser le caractère générique (`*`) à la place de chiffres dans un ID. Par exemple : **`m:vid-0781_pid-****;vid-0561_pid-554c`** La valeur par défaut n'est pas définie.
`Include Device Family`	Inclut des familles de périphériques pouvant être transmises. Le format du paramètre est {`m`|`o`}`:`*family_name_1*[`;`*family_name_2*]... Par exemple : **`m:storage`** La valeur par défaut n'est pas définie.
`Inclure un périphérique Vid/Pid`	Inclut des périphériques avec des ID de fournisseur et de produit spécifiés pouvant être transmis. Le format du paramètre est {`m`|`o`}`:vid-`*xxx1*`_pid-`*yyy2*[`;vid-`*xxx2*`_pid-`*yyy2*]... Vous devez spécifier des numéros d'ID au format hexadécimal. Vous pouvez utiliser le caractère générique (`*`) à la place de chiffres dans un ID. Par exemple : **`o:vid-0561_pid-554c`** La valeur par défaut n'est pas définie.

Tableau 8-7 décrit chaque paramètre de règle interprété par un client dans le fichier de modèle d'administration pour la configuration de View Agent. View Agent n'applique pas ces paramètres. View Agent transmet les paramètres à View Client pour interprétation et application. View Client utilise les paramètres pour décider si un périphérique USB est disponible pour la redirection.

Tableau 8-7. Modèle pour la configuration de View Agent : paramètres interprétés par un client

Paramètre	Propriétés
`Allow Audio Input Devices`	Permet la transmission de périphériques d'entrée audio. La valeur par défaut n'est pas définie.
`Allow Audio Output Devices`	Permet la transmission de périphériques de sortie audio. La valeur par défaut n'est pas définie.
`Allow HIDBootable`	Permet la transmission de périphériques d'entrée autres que des claviers et des souris qui sont disponibles au démarrage (ou périphériques démarrables par HID). La valeur par défaut n'est pas définie.

Tableau 8-7. Modèle pour la configuration de View Agent : paramètres interprétés par un client (suite)

Paramètre	Propriétés
`Autoriser d'autres périphériques d'entrée`	Permet la transmission de périphériques d'entrée autres que des périphériques démarrables par HID ou des claviers avec périphériques de pointage intégrés. La valeur par défaut n'est pas définie.
`Allow Keyboard and Mouse Devices`	Permet la transmission de claviers avec périphériques de pointage intégrés (souris, Trackball ou pavé tactile). La valeur par défaut n'est pas définie.
`Allow Smart Cards`	Permet la transmission de périphériques à carte à puce. La valeur par défaut n'est pas définie.
`Allow Video Devices`	Permet la transmission de périphériques vidéo. La valeur par défaut n'est pas définie.

Exécution de commandes sur des postes de travail View

Vous pouvez utiliser les paramètres de stratégie de groupe `CommandsToRunOnConnect` et `CommandsToRunOnReconnect` de View Agent pour exécuter des commandes et des scripts de commande sur des postes de travail View lorsque des utilisateurs se connectent et se reconnectent.

Pour exécuter une commande ou un script de commande, ajoutez le nom de commande ou le chemin de fichier du script à la liste de commandes du paramètre de stratégie de groupe. Par exemple :

```
date
```

```
C:\Scripts\myscript.cmd
```

Pour exécuter des scripts qui requièrent un accès à la console, ajoutez en préfixe l'option `–C` ou `–c` suivie d'un espace. Par exemple :

```
–c C:\Scripts\Cli_clip.cmd
```

```
–C e:\procexp.exe
```

Les types de fichiers pris en charge sont `.CMD`, `.BAT` et `.EXE`. Les fichiers `.VBS` ne sont pas exécutés sauf s'ils sont analysés avec `cscript.exe` ou `wscript.exe`. Par exemple :

```
–C C:\WINDOWS\system32\wscript.exe C:\Scripts\checking.vbs
```

La longueur totale de la chaîne, y compris l'option `–C` ou `–c`, ne doit pas dépasser 260 caractères.

Envoi d'informations sur le système client à des postes de travail View

Lorsqu'un utilisateur se connecte ou se reconnecte à un poste de travail View, le client View collecte des informations sur le système client et Serveur de connexion View envoie ces informations au poste de travail. View Agent écrit les informations sur l'ordinateur client dans le chemin `HKCU\Volatile Environment` du registre système du poste de travail.

Vous pouvez ajouter des commandes aux paramètres de stratégie de groupe `CommandsToRunOnConnect` et `CommandsToRunOnReconnect` de View Agent pour exécuter des commandes et des scripts de commande lisant ces informations dans le registre système lorsque des utilisateurs se connectent et se reconnectent à des postes de travail. Reportez-vous à la section « Exécution de commandes sur des postes de travail View », page 213 pour plus d'informations.

Tableau 8-8 décrit les clés de Registre qui contiennent des informations sur le système client et répertorie les types de systèmes client qui les prennent en charge.

Tableau 8-8. Informations sur le système client

Clé de Registre	Description	Systèmes client pris en charge
`ViewClient_IP_Address`	Adresse IP du système client.	Windows Linux Mac
`ViewClient_MAC_Address`	Adresse MAC du système client.	Windows Linux Mac
`ViewClient_Machine_Name`	Nom de machine du système client.	Windows Linux Mac
`ViewClient_Machine_Domain`	Domaine du système client.	Windows Linux Mac
`ViewClient_LoggedOn_Username`	Nom d'utilisateur utilisé pour se connecter au système client.	Windows Linux Mac
`ViewClient_LoggedOn_Domainname`	Nom de domaine utilisé pour se connecter au système client.	Windows **Remarque** Pour les clients Linux et Mac, voir `ViewClient_Machine_Domain`. `ViewClient_LoggedOn_Domainname` n'est pas donné par le client Linux ou Mac car les comptes Linux et Mac ne sont pas liés à des domaines Windows.
`ViewClient_Type`	Nom du client léger ou type de système d'exploitation du système client.	Windows Linux Mac
`ViewClient_Broker_DNS_Name`	Nom DNS de l'instance de Serveur de connexion View.	Windows Linux Mac
`ViewClient_Broker_URL`	URL de l'instance de Serveur de connexion View.	Windows Linux Mac
`ViewClient_Broker_Tunneled`	État de la connexion tunnel du serveur Serveur de connexion View qui peut être `true` (activé) ou `false` (désactivé).	Windows Linux Mac
`ViewClient_Broker_Tunnel_URL`	URL de la connexion tunnel de Serveur de connexion View, si la connexion tunnel est activée.	Windows Linux Mac
`ViewClient_Broker_Remote_IP_Address`	Adresse IP du système client qui est vue par l'instance de Serveur de connexion View.	Windows Linux Mac

Tableau 8-8. Informations sur le système client (suite)

Clé de Registre	Description	Systèmes client pris en charge
`ViewClient_TZID`	ID du fuseau horaire Olson. Pour désactiver la synchronisation du fuseau horaire, activez le paramètre de stratégie de groupe `Disable Time Zone Synchronization` de View Agent.	Windows Linux Mac
`ViewClient_Windows_Timezone`	Heure GMT standard. Pour désactiver la synchronisation du fuseau horaire, activez le paramètre de stratégie de groupe `Disable Time Zone Synchronization` de View Agent.	Windows

Paramètres de modèle d'administration pour la configuration de View Client

Le fichier de modèle d'administration pour la configuration de View Client (`vdm_client.adm`) contient des paramètres de stratégie liés à la configuration de View Client.

Paramètres de définition de script

Tableau 8-9 décrit les paramètres de définition de script dans le fichier de modèle d'administration pour la configuration de View Client. Le modèle fournit une version de Configuration d'ordinateur et de Configuration d'utilisateur de chaque paramètre de définition de script. Le paramètre de Configuration d'utilisateur remplace le paramètre de Configuration d'ordinateur équivalent.

Tableau 8-9. Modèle de configuration View Client : définitions de script

Paramètre	Description
`Connect all USB devices to the desktop on launch`	Détermine si tous les périphériques USB disponibles sur le système client sont connectés au poste de travail lorsque ce dernier est lancé.
`Connect all USB devices to the desktop when they are plugged in`	Détermine si les périphériques USB sont connectés au poste de travail lorsqu'ils sont branchés sur le système client.
`DesktopLayout`	Spécifie la disposition de la fenêtre View Client qu'un utilisateur voit lors de l'ouverture de session sur un poste de travail View. Les différentes dispositions sont les suivantes : ■ `Plein écran` ■ `Plusieurs écrans` ■ `Fenêtre – Grande` ■ `Fenêtre – Petite` Ce paramètre n'est disponible que lorsque le paramètre `Nom de poste de travail à sélectionner` est également défini.
`Nom de poste de travail à sélectionner`	Spécifie le poste de travail par défaut que View Client utilise lors de l'ouverture de session.
`Désactiver les plug-ins Terminal Services tiers`	Détermine si View Client vérifie les plug-ins Terminal Services tiers installés en tant que plug-ins RDP normaux. Si vous ne configurez pas ce paramètre, View Client vérifie les plug-ins tiers par défaut. Ce paramètre n'affecte pas les plug-ins spécifiques de View, comme la redirection USB.
`Nom de domaine d'ouverture de session`	Spécifie le domaine NetBIOS que View Client utilise lors de l'ouverture de session.
`Logon Password`	Spécifie le mot de passe que View Client utilise lors de l'ouverture de session. Active Directory stocke ce mot de passe en texte brut.
`Nom d'utilisateur d'ouverture de session`	Spécifie le nom d'utilisateur que View Client utilise lors de l'ouverture de session.

Tableau 8-9. Modèle de configuration View Client : définitions de script (suite)

Paramètre	Description
`Server URL`	Spécifie l'URL que View Client utilise lors de l'ouverture de session, par exemple, `http://view1.example.com`.
`Supprimer les messages d'erreur (lorsque entièrement scripté uniquement)`	Détermine si des messages d'erreur de View Client sont masqués lors de l'ouverture de session. Ce paramètre ne s'applique que lorsque le processus d'ouverture de session est entièrement scripté, par exemple, lorsque toutes les informations d'ouverture de session requises sont préremplies par la règle. Si l'ouverture de session échoue à cause d'informations d'ouverture de session erronées, l'utilisateur n'est pas informé et le processus `wswc.exe` de View Client est terminé.

Paramètres de sécurité

Tableau 8-10 décrit les paramètres de sécurité dans le fichier de modèle d'administration pour la configuration de View Client. Ce tableau montre si les paramètres incluent à la fois les paramètres Configuration ordinateur et Configuration utilisateur ou uniquement les paramètres Configuration ordinateur. Pour les paramètres de sécurité qui incluent les deux types, le paramètre Configuration utilisateur remplace le paramètre Configuration ordinateur équivalent.

Tableau 8-10. Modèle de configuration View Client : Paramètres de sécurité

Paramètre	Ordinateur	Utilisateur	Description
`Allow command line credentials`	X		Détermine si les informations d'identification d'utilisateur peuvent être fournies avec des options de ligne de commande View Client. Si ce paramètre est activé, les options `smartCardPIN` et `password` ne sont pas disponibles lorsque les utilisateurs exécutent View Client à partir de la ligne de commande. Ce paramètre est activé par défaut.
`Servers Trusted For Delegation`	X		Spécifie les instances de Serveur de connexion View qui acceptent l'identité et les informations d'identification d'utilisateur qui sont transmises quand un utilisateur coche la case **[Se connecter en tant qu'utilisateur actuel]**. Si vous ne spécifiez aucune instance de Serveur de connexion View, toutes les instances de Serveur de connexion View acceptent ces informations. Pour ajouter une instance de Serveur de connexion View, utilisez l'un des formats suivants : ■ **`domain\system$`** ■ **`system$@domain.com`** ■ Nom principal de service (SPN) du service Serveur de connexion View.

Tableau 8-10. Modèle de configuration View Client : Paramètres de sécurité (suite)

Paramètre	Ordinateur	Utilisateur	Description
`Certificate verification mode`	X		Configure le niveau de la vérification de certificat exécutée par View Client. Vous pouvez sélectionner l'un de ces modes : ■ `Pas de sécurité`. View n'effectue pas la vérification de certificat. ■ `Avertir, mais autoriser`. Lorsque les problèmes de certificat de serveur suivants se produisent, un avertissement s'affiche, mais l'utilisateur peut continuer à se connecter à Serveur de connexion View : ■ Un certificat auto-signé est fourni par View. Dans ce cas, il est acceptable si le nom de certificat ne correspond pas au nom de Serveur de connexion View fourni par l'utilisateur dans View Client. ■ Un certificat vérifiable qui a été configuré dans votre déploiement a expiré ou n'est pas encore valide.

Tableau 8-10. Modèle de configuration View Client : Paramètres de sécurité (suite)

Paramètre	Ordinateur	Utilisateur	Description
			Si une autre condition d'erreur de certificat se produit, View affiche une boîte de dialogue d'erreur et empêche l'utilisateur de se connecter à Serveur de connexion View. `Avertir, mais autoriser` est la valeur par défaut. ■ `Full Security`. Si une erreur de type de certificat se produit, l'utilisateur ne peut pas se connecter à Serveur de connexion View. View affiche des erreurs de certificat à l'utilisateur. Lorsque ce paramètre de stratégie de groupe est configuré, les utilisateurs peuvent voir le mode de vérification de certificat sélectionné dans View Client, mais ils ne peuvent pas configurer le paramètre. La boîte de dialogue de configuration SSL informe les utilisateurs que l'administrateur a verrouillé le paramètre. Lorsque ce paramètre n'est pas configuré ou est désactivé, les utilisateurs de View Client peuvent sélectionner un mode de vérification de certificat. Pour permettre à View Server de réaliser des vérifications de certificats fournis par un View Client, le View Client doit établir des connexions HTTPS avec l'hôte de Serveur de connexion View ou du serveur de sécurité. La vérification des certificats n'est pas prise en charge si vous déchargez SSL vers un serveur intermédiaire qui établit des connexions HTTP avec l'hôte de Serveur de connexion View ou du serveur de sécurité. Pour les clients Windows, si vous ne voulez pas configurer ce paramètre en tant que stratégie de groupe, vous pouvez également activer la vérification de certificat en ajoutant le nom de valeur `CertCheckMode` à l'une des clés de Registre suivantes sur l'ordinateur client : ■ Pour Windows 32 bits : `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security` ■ Pour Windows 64 bits : `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security` Utilisez les valeurs suivantes dans la clé de registre : ■ **`0`** implémente `Pas de sécurité`. ■ **`1`** implémente `Avertir, mais autoriser`. ■ **`2`** implémente `Full Security`. Si vous configurez le paramètre de stratégie de groupe et le paramètre `CertCheckMode` dans la clé de registre, le paramètre de stratégie de groupe est prioritaire sur la valeur de la clé de registre.

Tableau 8-10. Modèle de configuration View Client : Paramètres de sécurité (suite)

Paramètre	Ordinateur	Utilisateur	Description
`Default value of the 'Log in as current user' checkbox`	X	X	Spécifie la valeur par défaut de la case **[Se connecter en tant qu'utilisateur actuel]** dans la boîte de dialogue de connexion de View Client. Ce paramètre remplace la valeur par défaut spécifiée lors de l'installation de View Client. Si un utilisateur exécute View Client à partir de la ligne de commande et qu'il spécifie l'option `logInAsCurrentUser`, cette valeur remplace ce paramètre. Lorsque la case **[Se connecter en tant qu'utilisateur actuel]** est cochée, l'identité et les informations d'identification que l'utilisateur a fournies lors de l'ouverture de session sur le système client sont transmises à l'instance de Serveur de connexion View, puis au poste de travail View. Lorsque la case est décochée, les utilisateurs doivent fournir leur identité et leurs informations d'identification plusieurs fois avant de pouvoir accéder à un poste de travail View. Ce paramètre est désactivé par défaut.
`Display option to Log in as current user`	X	X	Détermine si la case **[Se connecter en tant qu'utilisateur actuel]** est visible dans la boîte de dialogue de connexion de View Client. Lorsque la case est visible, les utilisateurs peuvent la cocher ou la décocher et remplacer sa valeur par défaut. Lorsque la case est masquée, les utilisateurs ne peuvent pas remplacer sa valeur par défaut dans la boîte de dialogue de connexion de View Client. Vous pouvez spécifier la valeur par défaut de la case **[Se connecter en tant qu'utilisateur actuel]** en utilisant le paramètre de stratégie `Valeur par défaut de la case Se connecter en tant qu'utilisateur actuel`. Ce paramètre est activé par défaut.
`Enable jump list integration`	X		Détermine si une liste de raccourcis apparaît dans l'icône de View Client sur la barre des tâches de Windows 7 et des systèmes supérieurs. La liste de raccourcis permet aux utilisateurs de se connecter à des instances de Serveur de connexion View et des postes de travail View récents. Si View Client est partagé, il se peut que vous ne vouliez pas que les utilisateurs voient les noms des postes de travail récents. Vous pouvez désactiver la liste de raccourcis en désactivant ce paramètre. Ce paramètre est activé par défaut.
`Enable Single Sign-On for smart card authentication`	X		Détermine si l'authentification unique est activée pour l'authentification par carte à puce. Lorsque l'authentification unique est activée, View Client stocke le code PIN de carte à puce crypté dans la mémoire temporaire avant de le soumettre à Serveur de connexion View. Lorsque l'authentification unique est désactivée, View Client n'affiche pas de boîte de dialogue de code PIN personnalisé.

Tableau 8-10. Modèle de configuration View Client : Paramètres de sécurité (suite)

Paramètre	Ordinateur	Utilisateur	Description
`Ignore bad SSL certificate date received from the server`	X		Détermine si les erreurs associées aux dates des certificats de serveur non valides sont ignorées. Ces erreurs se produisent quand un serveur envoie un certificat avec une date passée. Ce paramètre s'applique uniquement à View 4.6 et versions antérieures.
`Ignore certificate revocation problems`	X		Détermine si les erreurs associées à un certificat de serveur révoqué sont ignorées. Ces erreurs se produisent lorsque le serveur envoie un certificat qui a été révoqué et lorsque le client ne peut pas vérifier l'état de révocation d'un certificat. Ce paramètre est désactivé par défaut. Ce paramètre s'applique uniquement à View 4.6 et versions antérieures.
`Ignore incorrect SSL certificate common name (host name field)`	X		Détermine si les erreurs associées à des noms communs de certificats de serveur incorrects sont ignorées. Ces erreurs se produisent quand le nom commun sur le certificat ne correspond pas au nom d'hôte du serveur qui l'envoie. Ce paramètre s'applique uniquement à View 4.6 et versions antérieures.
`Ignore incorrect usage problems`	X		Détermine si les erreurs associées à une utilisation incorrecte d'un certificat de serveur sont ignorées. Ces erreurs se produisent lorsque le serveur envoie un certificat ayant un autre but que vérifier l'identité de l'expéditeur et crypter les communications du serveur. Ce paramètre s'applique uniquement à View 4.6 et versions antérieures.
`Ignore unknown certificate authority problems`	X		Détermine si les erreurs associées à une autorité de certification inconnue sur le certificat du serveur sont ignorées. Ces erreurs se produisent lorsque le serveur envoie un certificat signé par une autorité tierce non approuvée. Ce paramètre s'applique uniquement à View 4.6 et versions antérieures.

paramètres RDP

Tableau 8-11 décrit les paramètres RDP (Remote Desktop Protocol) dans le fichier de modèle d'administration pour la configuration de View Client. Tous les paramètres RDP sont des paramètres de Configuration d'utilisateur.

Tableau 8-11. Modèle d'administration de configuration View Client : paramètres RDP

Paramètre	Description
`Redirection audio`	Détermine si les informations audio lues sur le poste de travail View sont redirigées. Sélectionnez l'un des paramètres suivants : **Disable Audio** — Les sons sont désactivés. **Play in VM (needed for VoIP USB Support)** — Les sons sont lus sur le poste de travail View. Ce paramètre requiert un périphérique audio USB partagé pour que le client reçoive le son. **Redirect to client** — Les sons sont redirigés vers le client. Il s'agit du mode par défaut. Ce paramètre ne s'applique qu'à l'audio RDP. Les sons redirigés via MMR sont lus sur le client.
`Audio capture redirection`	Détermine si le périphérique d'entrée audio par défaut est redirigé du client vers la session distante. Lorsque ce paramètre est activé, le périphérique d'enregistrement audio sur le client apparaît dans le poste de travail View et peut enregistrer une entrée audio. Le paramètre par défaut est désactivé.
`Bitmap cache file size in` *unit* `for` *number* `Taille du fichier de cache bitmap en <unit> pour <number> bpp bitmaps`	Spécifie la taille du cache bitmap, en kilo-octets ou en mégaoctets, à utiliser pour les paramètres de couleur bitmap d'un nombre de bits par pixel (bpp) spécifique. Des versions séparées de ce paramètre sont fournies pour les combinaisons unité/bpp suivantes : ■ Ko/8 bpp ■ Mo/8 bpp ■ Mo/16 bpp ■ Mo/24 bpp ■ Mo/32 bpp
`Bitmap caching/cache persistence active`	Détermine si la mise en cache permanente des bitmaps est utilisée (active). La mise en cache permanente des bitmaps peut améliorer les performances de votre ordinateur mais requiert plus d'espace disque.
`Profondeur des couleurs`	Spécifie la profondeur des couleurs du poste de travail View. Sélectionnez l'un des paramètres disponibles : ■ 8 bits ■ 15 bits ■ 16 bits ■ 24 bits ■ 32 bits Pour les systèmes Windows XP 24 bits, vous devez activer la règle Limiter le nombre maximal de couleurs dans **[Configuration d'ordinateur] > [Modèles administratifs] > [Composants Windows] > [Terminal Services]** et la définir sur 24 bits.
`Ombre du curseur`	Détermine si une ombre apparaît sous le curseur sur le poste de travail View.
`Arrière-plan du poste de travail`	Détermine si l'arrière-plan du poste de travail apparaît lorsque des clients se connectent à un poste de travail View.
`Composition du poste de travail`	(Windows Vista ou supérieur) Détermine si la composition du poste de travail est activée sur le poste de travail View. Lorsque la composition de poste de travail est activée, les fenêtres individuelles ne se dessinent plus sur l'écran ou sur le périphérique d'affichage principal comme c'était le cas dans les précédentes versions de Microsoft Windows. Le dessin est redirigé vers des surfaces non affichées à l'écran, en mémoire vidéo, qui sont ensuite rendues sous la forme d'une image de poste de travail et représentées à l'écran.

Tableau 8-11. Modèle d'administration de configuration View Client : paramètres RDP (suite)

Paramètre	Description
`Activer la compression`	Détermine si les données RDP sont compressées. Ce paramètre est activé par défaut.
`Activer le fournisseur de services de sécurité des informations d'identification`	Spécifie si la connexion de poste de travail View utilise l'authentification de niveau réseau (NLA ou Network Level Authentication). Sous Windows Vista, les connexions de poste de travail à distance requièrent la NLA par défaut. Si le système d'exploitation client requiert la NLA pour les connexions de poste de travail à distance, vous devez activer ce paramètre sans quoi View Client ne pourra pas se connecter au poste de travail View. En plus d'activer ce paramètre, vous devez également vérifier que les conditions suivantes sont satisfaites : ■ Le client et le système d'exploitation client prennent en charge la NLA. ■ Les connexions client directes sont activées pour l'instance de Serveur de connexion View. Les connexions par tunnel ne sont pas prises en charge avec la NLA.
`Activer la reconnexion automatique RDP`	Détermine si le composant client RDP tente de se reconnecter à un poste de travail View après un échec de connexion du protocole RDP. Ce paramètre n'a aucun effet si l'option **[Utiliser une connexion par tunnel sécurisé vers le poste de travail]** est activée dans View Administrator. Ce paramètre est désactivé par défaut. **Remarque** La reconnexion automatique RDP est prise en charge pour les postes de travail exécutant View Agent version 4.5 ou supérieure uniquement. Si un poste de travail possède une version antérieure de View Agent, certaines fonctions ne fonctionneront pas.
`Lissage des polices`	(Windows Vista ou supérieur) Détermine si l'anticrénelage est appliqué aux polices sur le poste de travail View.
`Animation du menu et fenêtre`	Détermine si l'animation des menus et des fenêtres est activée lorsque des clients se connectent à un poste de travail View.
`Rediriger le presse-papier`	Détermine si les informations de presse-papier locales sont redirigées lorsque des clients se connectent au poste de travail View.
`Rediriger les lecteurs`	Détermine si les lecteurs de disques locaux sont redirigés lorsque des clients se connectent au poste de travail View. Par défaut, les lecteurs locaux sont redirigés. L'activation de ce paramètre, ou le laisser non configuré, permet de copier des données entre le lecteur redirigé sur le poste de travail distant et le lecteur sur l'ordinateur client. Désactivez ce paramètre si autoriser des données à passer du poste de travail distant à des ordinateurs clients d'utilisateurs représente un risque de sécurité potentiel dans votre déploiement. Une autre approche consiste à désactiver la redirection de dossier dans la machine virtuelle de poste de travail distant en activant le paramètre de stratégie de groupe de Microsoft Windows, `Do not allow drive redirection`. Le paramètre `Redirect drives` ne s'applique qu'à RDP.
`Rediriger les imprimantes`	Détermine si les imprimantes locales sont redirigées lorsque des clients se connectent au poste de travail View.
`Rediriger les ports série`	Détermine si les ports COM locaux sont redirigés lorsque des clients se connectent au poste de travail View.
`Rediriger les cartes à puce`	Détermine si les cartes à puce locales sont redirigées lorsque des clients se connectent au poste de travail View. **Remarque** Ce paramètre s'applique aux connexions RDP et PCoIP.

Tableau 8-11. Modèle d'administration de configuration View Client : paramètres RDP (suite)

Paramètre	Description
Rediriger les périphériques prêts à l'emploi pris en charge	Détermine si les périphériques locaux de point de vente et prêts à l'emploi sont redirigés lorsque des clients se connectent au poste de travail View. Ce comportement est différent de la redirection gérée par le composant de redirection USB de View Agent.
Ombrer les bitmaps	Détermine si les bitmaps sont ombrés. Ce paramètre n'a pas d'effet en plein écran.
Afficher le contenu d'une fenêtre lorsque l'utilisateur le fait glisser	Détermine si le contenu des dossiers s'affiche lorsqu'un utilisateur les fait glisser vers un nouvel emplacement.
Thèmes	Détermine si les thèmes apparaissent lorsque des clients se connectent à un poste de travail View.
Redirection de combinaisons de clés Windows	Détermine où les combinaisons de clés Windows sont appliquées. Ce paramètre vous permet d'envoyer des combinaisons de clés à la machine virtuelle distante ou d'appliquer des combinaisons de clés localement. Si ce paramètre n'est pas configuré, les combinaisons de clés sont appliquées localement.

Paramètres généraux

Tableau 8-12 décrit les paramètres généraux dans le fichier de modèle d'administration pour la configuration de View Client. Les paramètres généraux incluent des paramètres de Configuration d'ordinateur et de Configuration d'utilisateur. Le paramètre de Configuration d'utilisateur remplace le paramètre de Configuration d'ordinateur équivalent.

Tableau 8-12. Modèle de configuration View Client : Paramètres généraux

Paramètre	Ordinateur	Utilisateur	Description
Toujours au premier plan		X	Détermine si la fenêtre View Client est toujours la fenêtre au premier plan. Activer ce paramètre empêche la barre des tâches de Windows d'apparaître sur la fenêtre View Client en plein écran. Ce paramètre est activé par défaut.
Default Exit Behavior For Local Mode Desktops		X	Contrôle le comportement de fermeture par défaut des postes de travail exécutés en mode local. Le paramètre par défaut est **[Arrêt]** , qui entraîne l'arrêt du système d'exploitation client.
Delay the start of replications when starting the View Client with Local Mode	X		Spécifie le nombre de secondes pendant lequel le début d'une réplication est retardé après le démarrage de View Client with Local Mode. Une réplication copie toutes les modifications dans des fichiers de poste de travail local vers le poste de travail distant correspondant. La prochaine réplication planifiée démarre à l'issue du délai. Les réplications se produisent à des intervalles que vous spécifiez dans des règles de mode local dans View Administrator. Par défaut, le délai est de 900 secondes (15 minutes).

Tableau 8-12. Modèle de configuration View Client : Paramètres généraux (suite)

Paramètre	Ordinateur	Utilisateur	Description
Détermine si VMware View Client doit utiliser le fichier proxy.pac	X		Détermine si View Client utilise un fichier PAC (Proxy Auto Config). L'activation de ce paramètre force View Client à utiliser un fichier PAC. Un fichier PAC (appelé communément `proxy.pac`) aide les navigateurs Web et d'autres agents d'utilisateur à trouver le serveur proxy approprié pour une demande particulière d'URL ou de site Web. Si vous activez ce paramètre sur une machine multicœur, l'application WinINet que View Client utilise pour rechercher des informations de serveur proxy peut se bloquer. Désactivez ce paramètre si ce problème se produit sur votre machine. Ce paramètre est désactivé par défaut. **Remarque** Ce paramètre ne s'applique qu'aux connexions directes. Il n'affecte pas les connexions par tunnel. Ce paramètre s'applique uniquement à View 4.6 et versions antérieures.
Désactiver le transfert de fuseau horaire	X		Détermine si la synchronisation de fuseau horaire entre le poste de travail View et le client connecté est désactivée.
Disable toast notifications			Détermine s'il est nécessaire de désactiver les notifications de toast dans View Client. Activez ce paramètre si vous ne voulez pas que l'utilisateur voie des notifications de toast dans le coin de l'écran. **Remarque** Si vous activez ce paramètre, l'utilisateur ne voit pas d'avertissement de 5 minutes lorsque la fonction Délai d'expiration de la session est active.
Ne pas vérifier l'alignement des écrans		X	Par défaut, le poste de travail client ne s'étend pas sur plusieurs écrans si la combinaison de ces derniers ne forme pas un rectangle exact lorsqu'ils sont combinés. Activez ce paramètre pour remplacer la valeur par défaut. Ce paramètre est désactivé par défaut.
Activer l'accélération multimédia		X	Détermine si la redirection multimédia (MMR) est activée sur le client. MMR ne fonctionne pas correctement si le matériel d'affichage vidéo de View Client ne prend pas en charge la superposition. La règle MMR ne s'applique pas aux sessions de poste de travail local.
Activer l'ombre		X	Détermine si la barre de menu ombre est affichée en haut de la fenêtre de View Client. Ce paramètre est activé par défaut. **Remarque** La barre de menu ombre est désactivée par défaut pour le mode kiosque.
Rediriger les lecteurs de carte à puce en mode local	X		Détermine si des lecteurs de carte à puce sont redirigés vers des postes de travail locaux. Les lecteurs sont partagés avec le système client. Ce paramètre est activé par défaut.
Liste d'adresses de proxy par tunnel	X		Spécifie une liste d'adresses de tunnel. Le serveur proxy n'est pas utilisé pour ces adresses. Utilisez un point-virgule (;) pour séparer plusieurs entrées.

Tableau 8-12. Modèle de configuration View Client : Paramètres généraux (suite)

Paramètre	Ordinateur	Utilisateur	Description
`URL de l'aide en ligne de View Client`	X		Spécifie une autre URL depuis laquelle View Client peut récupérer des pages d'aide. Ce paramètre est conçu pour être utilisé dans des environnements qui ne peuvent pas récupérer le système d'aide hébergé à distance car ils n'ont pas d'accès à Internet.
`Épingler l'ombre`		X	Détermine si l'épingle de l'ombre du haut de la fenêtre View Client est activée et détermine si le masquage automatique de la barre de menus ne se produit pas. Ce paramètre est sans effet si l'ombre est désactivée. Ce paramètre est activé par défaut.

Paramètres USB pour View Client

Vous pouvez définir des paramètres de règle USB pour View Agent et View Client pour Windows. Lors de la connexion, View Client télécharge les paramètres de règle USB depuis View Agent et les utilise avec les paramètres de règle USB de View Client afin de décider les périphériques qu'il va rendre disponible pour la redirection depuis la machine hôte.

Tableau 8-13 décrit chaque paramètre de règle pour fractionner des périphériques USB composites dans le fichier de modèle d'administration pour la configuration de View Client. Les paramètres s'appliquent au niveau de l'ordinateur. De préférence, View Client lit les paramètres depuis le GPO au niveau de l'ordinateur. Sinon, il les lit depuis le registre dans `HKLM\Software\Policies\VMware, Inc.\VMware VDM\Client\USB`. Pour voir une description de la façon dont View applique les règles pour le fractionnement de périphériques USB composites, reportez-vous à la section « Configuration de paramètres de règle de fractionnement de périphérique pour des périphériques USB composites », page 228.

Tableau 8-13. Modèle de configuration View Client : paramètres de fractionnement USB

Paramètre	Propriétés
`Autoriser le fractionnement automatique de périphérique`	Autorise le fractionnement automatique de périphériques USB composites. La valeur par défaut n'est pas définie, ce qui équivaut à **`false`**.
`Exclude Vid/Pid Device From Split`	Exclut un périphérique USB composite spécifié par des ID de fournisseur et de produit du fractionnement. Le format du paramètre est `vid-`*xxx1*`_pid-`*yyy2*`[;vid-`*xxx2*`_pid-`*yyy2*`]...` Vous devez spécifier des numéros d'ID au format hexadécimal. Vous pouvez utiliser le caractère générique (**`*`**) à la place de chiffres dans un ID. Par exemple : **`vid-0781_pid-55**`** La valeur par défaut n'est pas définie.
`Split Vid/Pid Device`	Traite les composants d'un périphérique USB composite spécifiés par des ID de fournisseur et de produit en tant que périphériques séparés. Le format du paramètre est `vid-`*xxxx*`_pid-`*yyyy*`(exintf:`*zz*`[;exintf:`*ww*` ])` Vous pouvez utiliser le mot-clé **`exintf`** pour exclure des composants de la redirection en spécifiant leur numéro d'interface. Vous devez spécifier les numéros d'ID au format hexadécimal et les numéros d'interface au format décimal en incluant les zéros à gauche. Vous pouvez utiliser le caractère générique (**`*`**) à la place de chiffres dans un ID. Par exemple : **`vid-0781_pid-554c(exintf:01;exintf:02)`** **Remarque** View n'inclut pas automatiquement les composants que vous n'avez pas explicitement exclus. Vous devez spécifier une règle de filtre telle que `Include Vid/Pid Device` pour inclure ces composants. La valeur par défaut n'est pas définie.

Tableau 8-14 décrit chaque paramètre de règle pour filtrer des périphériques USB dans le fichier de modèle d'administration pour la configuration de View Client. Les paramètres s'appliquent au niveau de l'ordinateur. De préférence, View Client lit les paramètres depuis le GPO au niveau de l'ordinateur. Sinon, il les lit depuis le registre dans `HKLM\Software\Policies\VMware, Inc.\VMware VDM\Client\USB`. Pour voir une description de la façon dont View applique les règles pour le filtrage de périphériques USB, reportez-vous à la section « Configuration de paramètres de règle de filtre pour des périphériques USB », page 231.

Tableau 8-14. Modèle de configuration View Client : paramètres de filtrage USB

Paramètre	Propriétés
`Allow Audio Input Devices`	Permet la redirection de périphériques d'entrée audio. La valeur par défaut n'est pas définie, ce qui équivaut à **`true`**.
`Allow Audio Output Devices`	Permet la redirection de périphériques de sortie audio. La valeur par défaut n'est pas définie, ce qui équivaut à **`false`**.
`Allow HIDBootable`	Permet la redirection de périphériques d'entrée autres que des claviers et des souris qui sont disponibles au démarrage (ou périphériques démarrables par HID). La valeur par défaut n'est pas définie, ce qui équivaut à **`true`**.
`Autoriser le comportement du descripteur de périphérique à sécurité intégrée`	Autorise la redirection des périphériques même si le client View ne parvient pas à obtenir les descripteurs de configuration/périphérique. Pour autoriser un périphérique même s'il échoue la configuration/description, incluez-le dans les filtres Include (Inclure), comme `IncludeVidPid` ou `IncludePath`. La valeur par défaut n'est pas définie, ce qui équivaut à **`false`**.
`Autoriser d'autres périphériques d'entrée`	Permet la redirection de périphériques d'entrée autres que des périphériques démarrables par HID ou des claviers avec périphériques de pointage intégrés. La valeur par défaut n'est pas définie, ce qui équivaut à **`true`**.
`Allow Keyboard and Mouse Devices`	Permet la redirection de claviers avec périphériques de pointage intégrés (souris, Trackball ou pavé tactile). La valeur par défaut n'est pas définie, ce qui équivaut à **`false`**.
`Allow Smart Cards`	Permet la redirection de périphériques à carte à puce. La valeur par défaut n'est pas définie, ce qui équivaut à **`false`**.
`Allow Video Devices`	Permet la redirection de périphériques vidéo. La valeur par défaut n'est pas définie, ce qui équivaut à **`true`**.
`Désactiver la configuration à distance`	Désactive l'utilisation de paramètres de View Agent lors de l'exécution du filtrage de périphérique USB. La valeur par défaut n'est pas définie, ce qui équivaut à **`false`**.
`Exclude All Devices`	Exclut tous les périphériques USB de la redirection. Si ce paramètre est défini sur **`true`**, vous pouvez utiliser d'autres paramètres de règle pour autoriser la redirection de périphériques spécifiques ou de familles de périphériques. Si ce paramètre est défini sur **`false`**, vous pouvez utiliser d'autres paramètres de règle pour empêcher la redirection de périphériques spécifiques ou de familles de périphériques. Si vous définissez la valeur de `Exclude All Devices` sur **`true`** sur View Agent, et si ce paramètre est transmis à View Client, le paramètre de View Agent remplace le paramètre de View Client. La valeur par défaut n'est pas définie, ce qui équivaut à **`false`**.
`Exclude Device Family`	Exclut des familles de périphériques de la redirection. Le format du paramètre est *family_name_1*[**`;`***family_name_2*]... Par exemple : **`bluetooth;smart-card`** Si vous avez activé le fractionnement automatique de périphérique, View examine la famille de périphériques de chaque interface d'un périphérique USB composite pour décider quelles interfaces doivent être exclues. Si vous avez désactivé le fractionnement automatique de périphérique, View examine la famille de périphérique de l'ensemble du périphérique USB composite. La valeur par défaut n'est pas définie.

Tableau 8-14. Modèle de configuration View Client : paramètres de filtrage USB (suite)

Paramètre	Propriétés
`Exclure un périphérique Vid/Pid`	Exclut des périphériques avec des ID de fournisseur et de produit spécifiés de la redirection. Le format du paramètre est `vid-`*xxx1*`_pid-`*yyy2*`[;vid-`*xxx2*`_pid-`*yyy2*`]...` Vous devez spécifier des numéros d'ID au format hexadécimal. Vous pouvez utiliser le caractère générique (`*`) à la place de chiffres dans un ID. Par exemple : **`vid-0781_pid-****;vid-0561_pid-554c`** La valeur par défaut n'est pas définie.
`Exclure un chemin d'accès`	Exclut des périphériques dans des chemins de concentrateur ou de port spécifiés de la redirection. Le format du paramètre est `bus-`*x1*`[/`*y1*`]...port-`*z1*`[;bus-`*x2*`[/`*y2*`]...port-`*z2*`]...` Vous devez spécifier des numéros de bus et de port au format hexadécimal. Vous ne pouvez pas utiliser le caractère générique dans les chemins. Par exemple : **`bus-1/2/3_port-02;bus-1/1/1/4_port-ff`** La valeur par défaut n'est pas définie.
`Include Device Family`	Inclut des familles de périphériques pouvant être redirigées. Le format du paramètre est *family_name_1*`[;`*family_name_2*`]...` Par exemple : **`storage`** La valeur par défaut n'est pas définie.
`Inclure un chemin d'accès`	Inclut des périphériques dans des chemins de concentrateur ou de port spécifiés pouvant être redirigés. Le format du paramètre est `bus-`*x1*`[/`*y1*`]...port-`*z1*`[;bus-`*x2*`[/`*y2*`]...port-`*z2*`]...` Vous devez spécifier des numéros de bus et de port au format hexadécimal. Vous ne pouvez pas utiliser le caractère générique dans les chemins. Par exemple : **`bus-1/2_port-02;bus-1/7/1/4_port-0f`** La valeur par défaut n'est pas définie.
`Inclure un périphérique Vid/Pid`	Inclut des périphériques avec des ID de fournisseur et de produit spécifiés pouvant être redirigés. Le format du paramètre est `vid-`*xxx1*`_pid-`*yyy2*`[;vid-`*xxx2*`_pid-`*yyy2*`]...` Vous devez spécifier des numéros d'ID au format hexadécimal. Vous pouvez utiliser le caractère générique (`*`) à la place de chiffres dans un ID. Par exemple : **`vid-0561_pid-554c`** La valeur par défaut n'est pas définie.

Utilisation de règles pour contrôler la redirection USB

Vous pouvez configurer des règles USB pour View Agent et View Client pour Windows afin de spécifier si View Client doit fractionner des périphériques USB composites en composants séparés pour la redirection ; limiter les types de périphériques USB que View Client rend disponibles pour la redirection ; et demander à View Agent d'empêcher le transfert de certains périphériques USB depuis un ordinateur client. Vous ne pouvez pas utiliser de règles USB pour contrôler les périphériques USB pouvant être utilisés avec un poste de travail distant emprunté.

Si des versions antérieures de View Agent ou de View Client sont installées, toutes les fonctions des règles de redirection USB ne sont pas disponibles. Tableau 8-15 indique comment View applique les règles pour différentes combinaisons de View Agent et View Client pour Windows.

Tableau 8-15. Compatibilité des paramètres de règle USB

Version de View Agent	Version de View Client	Effet des paramètres de règle USB sur la redirection USB
5.1 ou version supérieure	5.1 ou version supérieure	Les paramètres de règle USB sont applicables sur View Agent et View Client. Vous pouvez utiliser des paramètres de règle USB de View Agent pour bloquer le transfert de périphériques USB vers un poste de travail. View Agent peut envoyer des paramètres de règle de fractionnement de périphérique et de filtrage à View Client. Vous pouvez utiliser des paramètres de règle USB de View Client pour empêcher la redirection de périphériques USB depuis un ordinateur client vers un poste de travail.
5.1 ou version supérieure	5.0.x ou antérieur	Les paramètres de règle USB s'appliquent uniquement à View Agent. Vous pouvez utiliser des paramètres de règle USB de View Agent pour bloquer le transfert de périphériques USB vers un poste de travail. Vous ne pouvez pas utiliser des paramètres de règle USB de View Client pour contrôler les périphériques pouvant être redirigés depuis un ordinateur client vers un poste de travail. View Client ne peut pas recevoir de paramètres de règle de fractionnement de périphérique et de filtrage de View Agent. Les paramètres de registre existants pour la redirection USB par View Client restent valides.
5.0.x ou antérieur	5.1 ou version supérieure	Les paramètres de règle USB s'appliquent uniquement à View Client. Vous pouvez utiliser des paramètres de règle USB de View Client pour empêcher la redirection de périphériques USB depuis un ordinateur client vers un poste de travail. Vous ne pouvez pas utiliser des paramètres de règle USB de View Agent pour bloquer le transfert de périphériques USB vers un poste de travail. View Agent ne peut pas envoyer des paramètres de règle de fractionnement de périphérique et de filtrage à View Client.
5.0.x ou antérieur	5.0.x ou antérieur	Les paramètres de règle USB ne s'appliquent pas. Les paramètres de registre existants pour la redirection USB par View Client restent valides.

Si vous mettez à niveau View Client, tous les paramètres de registre existants pour la redirection USB, tels que `HardwareIdFilters`, restent valides jusqu'à ce que vous définissiez des règles USB pour View Client.

Le client Linux ne prend pas en charge les règles USB. Vous pouvez utiliser les règles USB pour que View Agent contrôle les périphériques USB dont le transfert est autorisé d'un client Linux vers un poste de travail.

Configuration de paramètres de règle de fractionnement de périphérique pour des périphériques USB composites

Les périphériques USB composites sont constitués d'une combinaison de deux périphériques différents ou plus, tels qu'un périphérique de pointage et un périphérique d'entrée audio, un périphérique d'entrée vidéo et un périphérique de stockage, ou un périphérique de communications et un périphérique de stockage. Si vous voulez qu'un ou plusieurs des composants soient disponibles pour la redirection, vous pouvez fractionner le périphérique composite en interfaces de composant, exclure certaines interfaces de la redirection et créer un filtre séparé pour chaque interface.

Le Tableau 8-16 indique comment la valeur du paramètre `Allow Auto Device Splitting` détermine si View Client tente de fractionner des périphériques USB composites automatiquement. Par défaut, le fractionnement automatique est désactivé.

Tableau 8-16. Effet de la combinaison de règles de désactivation du fractionnement automatique

Règle Autoriser le fractionnement automatique de périphérique sur View Agent	Règle Autoriser le fractionnement automatique de périphérique sur View Client	Règle Autoriser le fractionnement automatique de périphérique effective combinée
`Allow – Default Client Setting`	**`false`** (fractionnement automatique désactivé)	Fractionnement automatique désactivé
`Allow – Default Client Setting`	**`true`** (fractionnement automatique activé)	Fractionnement automatique activé
`Allow – Default Client Setting`	Non défini	Fractionnement automatique activé

Tableau 8-16. Effet de la combinaison de règles de désactivation du fractionnement automatique (suite)

Règle Autoriser le fractionnement automatique de périphérique sur View Agent	Règle Autoriser le fractionnement automatique de périphérique sur View Client	Règle Autoriser le fractionnement automatique de périphérique effective combinée
`Allow – Override Client Setting`	Aucun ou non défini	Fractionnement automatique activé
Non défini	Non défini	Fractionnement automatique désactivé

Par défaut, View désactive le fractionnement automatique et exclut de la redirection tous les composants de sortie audio, de carte à puce, clavier ou souris d'un périphérique USB composite.

View applique les paramètres de règle de fractionnement de périphériques avant d'appliquer des paramètres de règle de filtre. Si vous avez activé le fractionnement automatique et si vous n'excluez pas explicitement un périphérique USB composite du fractionnement en spécifiant ses ID de fournisseur et de produit, View examine chaque interface du périphérique USB composite afin de décider quelles interfaces doivent être exclues ou incluses en fonction des paramètres de règle de filtre. Si vous avez désactivé le fractionnement automatique de périphérique et si vous ne spécifiez pas explicitement les ID de fournisseur et de produit d'un périphérique USB composite que vous voulez fractionner, View applique les paramètres de règle de filtre à l'ensemble du périphérique.

Si vous activez le fractionnement automatique, vous pouvez utiliser la règle `Exclude Vid/Pid Device From Split` pour spécifier les périphériques USB composites que vous voulez exclure du fractionnement.

Vous pouvez utiliser la règle `Split Vid/Pid Device` pour spécifier les ID de fournisseur et de produit d'un périphérique USB composite que vous voulez fractionner. Vous pouvez également spécifier les interfaces des composants d'un périphérique USB composite que vous voulez exclure de la redirection. View n'applique aucun paramètre de règle de filtre aux composants que vous excluez de cette façon.

IMPORTANT Si vous utilisez la règle `Split Vid/Pid Device`, View n'inclut pas automatiquement les composants que vous n'avez pas explicitement exclus. Vous devez spécifier une règle de filtre telle que `Include Vid/Pid Device` pour inclure ces composants.

Tableau 8-17 indique les modificateurs qui spécifient la façon dont View Client traite un paramètre de règle de fractionnement de périphérique de View Agent s'il existe un paramètre de règle de fractionnement de périphérique équivalent pour View Client. Ces modificateurs s'appliquent à tous les paramètres de règles de fractionnement de périphérique.

Tableau 8-17. Modificateurs de fractionnement pour des paramètres de règle de fractionnement de périphérique sur View Agent

Modificateur	Description
`m` (fusionner)	View Client applique le paramètre de règle de fractionnement de périphérique de View Agent en plus du paramètre de règle de fractionnement de périphérique de View Client.
`o` (remplacer)	View Client utilise le paramètre de règle de fractionnement de périphérique de View Agent au lieu du paramètre de règle de fractionnement de périphérique de View Client.

Le Tableau 8-18 montre des exemples de la façon dont View Client traite les paramètres pour `Exclude Device From Split by Vendor/Product ID` lorsque vous spécifiez différents modificateurs de fractionnement.

Tableau 8-18. Exemples d'application de modificateurs de fractionnement sur des paramètres de règle de fractionnement de périphérique

Exclure le périphérique du fractionnement par ID de fournisseur/produit sur View Agent	Exclure le périphérique du fractionnement par ID de fournisseur/produit sur View Client	Paramètre de règle Exclure le périphérique du fractionnement par ID de fournisseur/produit effectif utilisé par View Client
`m:vid-XXXX_pid-XXXX`	`vid-YYYY_pid-YYYY`	`vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY`
`o:vid-XXXX_pid-XXXX`	`vid-YYYY_pid-YYYY`	`vid-XXXX_pid-XXXX`
`m:vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY`	`vid-YYYY_pid-YYYY`	`vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY`
`o:vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY`	`vid-YYYY_pid-YYYY`	`vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY`

View Agent n'applique pas les paramètres de règle de fractionnement de périphérique de son côté de la connexion.

View Client évalue les paramètres de règle de fractionnement de périphérique dans l'ordre de priorité suivant.

- `Exclude Vid/Pid Device From Split`
- `Split Vid/Pid Device`

Un paramètre de règle de fractionnement de périphérique qui exclut un périphérique du fractionnement est prioritaire sur tout autre paramètre de règle pour fractionner le périphérique. Si vous définissez des interfaces ou des périphériques à exclure du fractionnement, View Client exclut les périphériques composants correspondant de la redirection.

Exemples de définition de règles pour fractionner des périphériques USB composites

Définissez des règles de fractionnement pour des postes de travail afin d'exclure des périphériques avec des ID de fournisseur et de produit spécifiques de la redirection après le fractionnement automatique et transmettre ces règles à des ordinateurs client.

Tableau 8-19. Utiliser des règles View Agent pour spécifier des paramètres de règle de fractionnement de périphérique

Règles de fractionnement USB sur View Agent	Règles de fractionnement USB sur View Client
`Exclude VidPid From Split` défini sur **`o:vid-xxxx_pid-yyyy`**. `Allow Auto Device Splitting` défini sur `Allow - Override Client Setting`.	Tous les paramètres pour `Allow Auto Device Splitting` et `Exclude VidPid From Split` sur View Client sont remplacés par View Agent.

Autorisez le fractionnement automatique de périphérique pour des postes de travail et spécifiez des règles pour fractionner des périphériques spécifiés sur des ordinateurs client.

Tableau 8-20. Utiliser des règles View Agent et View Client pour spécifier des paramètres de règle de fractionnement de périphérique

Règles de fractionnement USB sur View Agent	Règles de fractionnement USB sur View Client
`Allow Auto Device Splitting` défini sur `Allow – Override Client Setting`.	Le paramètre pour `Allow Auto Device Splitting` sur View Client est remplacé par View Agent. `Split Vid/Pid Device` défini sur **`vid-0781_pid-554c(exintf:00;exintf:01)`** pour fractionner un périphérique USB composite spécifié et exclure l'interface 00 et l'interface 01 de la redirection. REMARQUE Vous devez également spécifier une règle de filtre telle que `Include Vid/Pid Device` définie sur **`vid-0781_pid-554c`**, ce qui permet à View Client de rediriger les autres composants du périphérique.

Configuration de paramètres de règle de filtre pour des périphériques USB

Les paramètres de règle de filtre que vous configurez pour View Agent et View Client établissent les périphériques USB pouvant être redirigés depuis un ordinateur client vers un poste de travail.

Vous pouvez configurer des paramètres de règle de filtre de périphérique USB dans les paramètres de règle de View Agent et View Client. Lorsque vous vous connectez à un poste de travail, View Client télécharge les paramètres de règle USB de View Agent et les utilise avec les paramètres de règle USB de View Client afin de décider quels périphériques USB il va vous autoriser à rediriger depuis l'ordinateur client.

View applique tous les paramètres de règle de fractionnement de périphérique avant d'appliquer les paramètres de règle de filtre. Si vous avez fractionné un périphérique USB composite, View examine les interfaces de chaque périphérique afin de décider lesquelles doivent être exclues ou incluses en fonction des paramètres de règle de filtre. Si vous n'avez pas fractionné de périphérique USB composite, View applique les paramètres de règle de filtre à l'ensemble du périphérique.

Tableau 8-21 indique les modificateurs qui spécifient comment View Client gère un paramètre de règle de filtre View Agent pour un paramètre exécutable par un agent si un paramètre de règle de filtre équivalent existe pour View Client.

Tableau 8-21. Modificateurs de filtre pour des paramètres exécutables par un agent

Modificateur	Description
`m` (fusionner)	View Client applique le paramètre de règle de filtre de View Agent en plus du paramètre de règle de filtre de View Client.
`o` (remplacer)	View Client utilise le paramètre de règle de filtre de View Agent au lieu du paramètre de règle de filtre de View Client.

Tableau 8-22 montre des exemples de la façon dont View Client traite les paramètres pour `Exclude Vid/Pid Device` lorsque vous spécifiez différents modificateurs de filtre.

Tableau 8-22. Exemples d'application de modificateurs de filtre sur des paramètres exécutables par un agent

Paramètre Exclure un périphérique Vid/Pid sur View Agent	Paramètre Exclure un périphérique Vid/Pid sur View Client	Paramètre de règle Exclure un périphérique Vid/Pid effectif utilisé par View Client
`o:vid-0a34_pid-****`	**`vid-0122_pid-5cce`**	**`vid-0a34_pid-****`**
`m:vid-0a34_pid-****`	**`vid-0122_pid-5cce`**	**`vid-0a34_pid-****;vid-0122_pid-5cce`**

Tableau 8-23 indique les modificateurs qui spécifient la façon dont View Client traite un paramètre de règle de filtre de View Agent pour un paramètre interprété par un client.

Tableau 8-23. Modificateurs de filtre pour des paramètres interprétés par un client

Modificateur	Description
`Default` (**d** dans le paramètre de registre)	Si un paramètre de règle de filtre de View Client n'existe pas, View Client utilise le paramètre de règle de filtre de View Agent. Si un paramètre de règle de filtre de View Client existe, View Client applique ce paramètre de règle et ignore le paramètre de règle de filtre de View Agent.
`Override` (**o** dans le paramètre de registre)	View Client utilise le paramètre de règle de filtre de View Agent au lieu d'un paramètre de règle de filtre de View Client équivalent.

View Agent n'applique pas les paramètres de règle de filtre pour des paramètres interprétés par un client de son côté de la connexion.

Tableau 8-24 montre des exemples de la façon dont View Client traite les paramètres pour `Allow Smart Cards` lorsque vous spécifiez différents modificateurs de filtre.

Tableau 8-24. Exemples d'application de modificateurs de filtre sur des paramètres interprétés par un client

Paramètre Autoriser les cartes à puce sur View Agent	Paramètre Autoriser les cartes à puce sur View Client	Paramètre de règle Autoriser les cartes à puce effectif utilisé par View Client
`Disable – Default Client Setting` (**d:false** dans le paramètre de registre)	**true** (autoriser)	**true** (autoriser)
`Disable – Override Client Setting` (**o:false** dans le paramètre de registre)	**true** (autoriser)	**false** (désactiver)

Si vous définissez la règle `Disable Remote Configuration Download` sur **true**, View Client ignore tous les paramètres de règle de filtre qu'il reçoit de View Agent.

View Agent applique toujours les paramètres de règle de filtre dans les paramètres exécutables par un agent de son côté de la connexion même si vous configurez View Client afin qu'il utilise un paramètre de règle de filtre différent ou si vous empêchez View Client de télécharger des paramètres de règle de filtre depuis View Agent. View Client ne signale pas que View Agent bloque le transfert d'un périphérique.

Si vous définissez la règle `Exclude All Devices` sur **true**, View Client empêche la redirection de tous les périphériques USB. Vous pouvez utiliser d'autres paramètres de règle pour autoriser la redirection de périphériques spécifiques ou de familles de périphériques. Si vous définissez la règle sur **false**, View Client autorise la redirection de tous les périphériques USB sauf ceux qui sont bloqués par d'autres paramètres de règle. Vous pouvez définir la règle sur View Agent et sur View Client. Tableau 8-25 indique comment la règle `Exclude All Devices` que vous pouvez définir pour View Agent et View Client se combine pour produire une règle effective pour l'ordinateur client. Par défaut, tous les périphériques USB sont autorisés à être redirigés, sauf blocage contraire.

Tableau 8-25. Effet de la combinaison de règles Exclure tous les périphériques

Règle Exclure tous les périphériques sur View Agent	Règle Exclure tous les périphériques sur View Client	Règle Exclure tous les périphériques effective combinée
false ou non défini (inclure tous les périphériques USB)	**false** ou non défini (inclure tous les périphériques USB)	Inclure tous les périphériques USB
false (inclure tous les périphériques USB)	**true** (exclure tous les périphériques USB)	Exclure tous les périphériques USB
true (exclure tous les périphériques USB)	Aucun ou non défini	Exclure tous les périphériques USB

Si vous avez défini la règle `Disable Remote Configuration Download` sur **`true`**, la valeur de `Exclude All Devices` sur View Agent n'est pas transmise à View Client, mais View Agent et View Client appliquent la valeur locale de `Exclude All Devices`.

View Client évalue les paramètres de règle de filtre selon un ordre de priorité. Un paramètre de règle de filtre qui exclut la redirection d'un périphérique correspondant est prioritaire sur le paramètre de règle de filtre équivalent qui inclut le périphérique. Si View Client ne trouve pas de paramètre de règle de filtre pour exclure un périphérique, View Client autorise la redirection du périphérique sauf si vous avez défini la règle `Exclude All Devices` sur **`true`**. Toutefois, si vous avez configuré un paramètre de règle de filtre sur View Agent afin d'exclure le périphérique, le poste de travail bloque toute tentative de redirection du périphérique sur lui.

View Client évalue les paramètres de règle de filtre dans l'ordre de priorité suivant en prenant en compte les paramètres de View Client et les paramètres de View Agent, ainsi que les valeurs de modificateur que vous appliquez aux paramètres de View Agent.

- `Exclure un chemin d'accès`
- `Inclure un chemin d'accès`
- `Exclure un périphérique Vid/Pid`
- `Inclure un périphérique Vid/Pid`
- `Exclude Device Family`
- `Include Device Family`
- `Allow Audio Input Devices`, `Allow Audio Output Devices`, `Allow HIDBootable`, `Allow HID (Non Bootable and Not Mouse Keyboard)`, `Allow Keyboard and Mouse Devices`, `Allow Smart Cards` et `Allow Video Devices`
- Règle `Exclude All Devices` effective combinée évaluée pour exclure ou inclure tous les périphériques USB

Vous pouvez définir les paramètres de règle de filtre `Exclude Path` et `Include Path` uniquement pour View Client. Les paramètres de règle de filtre `Allow` qui font référence à des familles de périphériques séparés ont la même priorité.

Si vous configurez un paramètre de règle pour exclure des périphériques en fonction de valeurs d'ID de fournisseur et de produit, View Client exclut un périphérique dont les valeurs d'ID de fournisseur et de produit correspondent à ce paramètre de règle même si vous pouvez avoir configuré un paramètre de règle `Allow` pour la famille à laquelle le périphérique appartient.

L'ordre de priorité des paramètres de règle résout des conflits entre les paramètres de règle. Si vous configurez `Allow Smart Cards` pour autoriser la redirection de cartes à puce, tout paramètre de règle d'exclusion avec une priorité supérieure remplace ce paramètre. Par exemple, vous pouvez avoir configuré un paramètre de règle `Exclude Vid/Pid Device` pour exclure les périphériques à carte à puce avec un chemin ou des valeurs d'ID de fournisseur et de produit correspondants, ou vous pouvez avoir configuré un paramètre de règle `Exclude Device Family` qui exclut également la famille de périphériques `smart-card` entièrement.

Si vous avez configuré des paramètres de règle de filtre View Agent, View Agent évalue et applique les paramètres de règle de filtre dans l'ordre de priorité suivant sur le poste de travail.

- `Exclure un périphérique Vid/Pid`
- `Inclure un périphérique Vid/Pid`
- `Exclude Device Family`
- `Include Device Family`
- Règle `Exclude All Devices` appliquée par un agent définie pour exclure ou inclure tous les périphériques USB

View Agent applique cet ensemble limité de paramètres de règle de filtre de son côté de la connexion.

En définissant des paramètres de règle de filtre pour View Agent, vous pouvez créer un paramètre de filtrage pour des ordinateurs client non gérés. La fonction vous permet également de bloquer le transfert de périphériques depuis des ordinateurs client, même si les paramètres de règle de filtre pour View Client autorisent la redirection.

Par exemple, si vous configurez une règle qui permet à View Client d'autoriser la redirection d'un périphérique, View Agent bloque le périphérique si vous configurez une règle pour que View Agent exclue le périphérique.

Exemples de définition de règles pour filtrer des périphériques USB

Limitez les postes de travail afin qu'ils autorisent des ordinateurs client à transmettre uniquement des périphériques de stockage.

Tableau 8-26. Bloquer tous les périphériques USB sauf les périphériques de stockage

Règles de filtrage USB sur View Agent	Règles de filtrage USB sur View Client
`Include Device Family` défini sur **`o:storage`**. `Exclude All Devices` défini sur **`true`**.	Tout paramètre de `Include Device Family` ou `Exclude All Devices` sur View Client est remplacé.

Limitez les postes de travail afin qu'ils autorisent les ordinateurs client à transmettre uniquement les périphériques avec des valeurs d'ID de fournisseur et de produit qui correspondent à un mode spécifié.

Tableau 8-27. Bloquer tous les périphériques USB sauf les périphériques avec des valeurs d'ID de fournisseur et de produit spécifiées

Règles de filtrage USB sur View Agent	Règles de filtrage USB sur View Client
`Include Vid/Pid Device` défini sur **`o:vid-0561_pid-554c;vid-0781_pid-****`**. `Exclude All Devices` défini sur **`true`**.	Tout paramètre de `Include Vid/Pid Device` ou `Exclude All Devices` sur View Client est remplacé.

Autorisez les ordinateurs client à rediriger tous les périphériques à l'exception des périphériques à carte à puce et des périphériques démarrables par HID.

Tableau 8-28. Autoriser la redirection de tous les périphériques USB sauf les périphériques à carte à puce et les périphériques démarrables par HID

Règles USB sur View Agent	Règles USB sur View Client
`Exclude All Devices` défini sur **`false`**.	`Allow Smartcard` défini sur **`false`**. `Allow HIDBootable` défini sur **`false`**.

Familles de périphériques USB

Vous pouvez spécifier une famille lorsque vous créez des règles de filtrage USB pour View Client ou View Agent.

Tableau 8-29. Familles de périphériques USB

Nom de la famille de périphériques	Description
`audio`	Tout périphérique d'entrée ou de sortie audio.
`audio-in`	Périphériques d'entrée audio, tels que des microphones.
`audio-out`	Périphériques de sortie audio, tels que des haut-parleurs et des écouteurs.
`bluetooth`	Périphériques connectés par Bluetooth.
`comm`	Périphériques de communication, tels que des modems et des adaptateurs réseau filaires.
`hid`	Périphériques d'interface humaine, à l'exclusion des claviers et des pointeurs.

Tableau 8-29. Familles de périphériques USB (suite)

Nom de la famille de périphériques	Description
`hid-bootable`	Périphériques d'interface humaine disponibles au démarrage, à l'exclusion des claviers et des pointeurs.
`imaging`	Périphériques graphiques tels que des scanners.
`keyboard`	Périphérique de type clavier.
`mouse`	Périphérique de pointage tel qu'une souris.
`other`	Famille non spécifiée.
`pda`	Assistants numériques personnels.
`physical`	Périphériques à retour de force, tels que les joysticks à retour de force.
`printer`	Périphériques d'impression.
`security`	Périphériques de sécurité, tels que des lecteurs d'empreintes digitales.
`smart-card`	Périphériques à carte à puce.
`storage`	Périphériques de stockage de masse tels que des disques à mémoire flash et des disques durs externes.
`unknown`	Famille inconnue.
`vendor`	Périphériques disposant de fonctions spécifiques au fournisseur.
`video`	Périphériques d'entrée vidéo.
`wireless`	Adaptateurs réseau sans fil.
`wusb`	Périphériques USB sans fil.

Remarque Pour les versions antérieures à 5.1, View Client pour Windows lit la famille du périphérique sur le pilote du périphérique que vous avez installé sur l'ordinateur client. Pour View 5.1, il n'est pas nécessaire d'installer le pilote du périphérique sur un ordinateur client Windows. View Client lit la famille du périphérique sur le périphérique lui-même et pas sur le pilote du périphérique. Le micrologiciel d'un périphérique USB définit généralement la famille du périphérique, ce qui décrit sa fonction, même si tous les périphériques n'indiquent pas la valeur correcte correspondant à la famille.

Les clients légers basés sur Linux lisent toujours la famille du périphérique sur le périphérique lui-même.

Paramètres de modèle d'administration pour la configuration de View Server

Le fichier de modèle d'administration pour la configuration de View Server (`vdm_server.adm`) contient des paramètres de stratégie liés à View Connection Server.

Tableau 8-30 décrit chaque paramètre de stratégie dans le fichier de modèle d'administration pour la configuration de View Server. Le modèle ne contient que des paramètres de Configuration d'ordinateur.

Tableau 8-30. Paramètres de modèle pour la configuration de View Server

Paramètre	Propriétés
`Recursive Enumeration of Trusted Domains (Énumération récursive de domaines approuvés)`	Détermine si le domaine dans lequel le serveur réside énumère chaque domaine approuvé. Pour établir une chaîne de confiance complète, les domaines approuvés par chaque domaine approuvé sont aussi énumérés et le processus continue récursivement jusqu'à ce que tous les domaines approuvés soient détectés. Ces informations sont transmises à View Connection Server pour que le client dispose de tous les domaines approuvés lors des ouvertures de session. Ce paramètre est activé par défaut. Lorsqu'il est désactivé, seuls les domaines approuvés directement sont énumérés et la connexion aux contrôleurs de domaine distants n'est pas assurée. Dans des environnements contenant des relations de domaine complexes (telles que celles utilisant plusieurs structures de forêt avec approbations entre domaines de leurs forêts), ce processus peut prendre plusieurs minutes.

Paramètres de modèle d'administration pour la configuration commune de View

Le fichier de modèle d'administration pour la configuration commune de View (`vdm_common.adm`) contient des paramètres de stratégie communs à tous les composants View. Ce modèle ne contient que des paramètres de Configuration d'ordinateur.

paramètres de configuration de journal

Tableau 8-31 décrit chaque paramètre de stratégie pour la configuration de journal dans le fichier de modèle d'administration pour la configuration commune de View.

Tableau 8-31. Modèle de configuration commune de View : paramètres de configuration de journal

Paramètre	Propriétés
`Number of days to keep production logs (Nombre de jours de conservation des journaux de production)`	Spécifie le nombre de jours pendant lesquels les fichiers journaux sont conservés sur le système. Si vous ne définissez pas de valeur, la valeur par défaut s'applique et les fichiers journaux sont conservés sept jours.
`Maximum number of debug logs (Nombre maximum de journaux de débogage)`	Spécifie le nombre maximum de fichiers journaux de débogage à conserver sur le système. Lorsqu'un fichier journal atteint sa taille maximale, aucune nouvelle entrée n'est ajoutée et un nouveau fichier journal est créé. Lorsque le nombre de fichiers journaux précédents atteint cette valeur, le fichier journal le plus ancien est supprimé.
`Maximum debug log size in Megabytes (Taille maximale des journaux de débogage en mégaoctets)`	Spécifie la taille maximale en mégaoctets qu'un journal de débogage peut atteindre avant que le fichier journal ne soit fermé et qu'un nouveau fichier journal ne soit créé.
`Log Directory (Répertoire des journaux)`	Spécifie le chemin complet vers le répertoire pour les fichiers journaux. Si l'emplacement n'est pas inscriptible, l'emplacement par défaut est utilisé. Pour les fichiers journaux client, un répertoire supplémentaire avec le nom de client est créé.

paramètres d'alarme de performance

Tableau 8-32 décrit les paramètres d'alarme de performance dans le fichier de modèle d'administration pour la configuration commune de View.

Tableau 8-32. Modèle de configuration commune de View : paramètres d'alarme de performance

Paramètre	Propriétés
`CPU and Memory Sampling Interval in Seconds (Intervalle d'échantillonnage de mémoire et de CPU en secondes)`	Spécifie le CPU et le CPU d'intervalle d'interrogation de la mémoire. Un intervalle d'échantillonnage faible peut entraîner un niveau élevé de sortie vers le journal.
`Overall CPU usage percentage to issue log info (Pourcentage d'utilisation du CPU global pour émettre des informations de journalisation)`	Spécifie le seuil auquel l'utilisation du CPU global du système est journalisée. Lorsque plusieurs processeurs sont disponibles, ce pourcentage représente l'utilisation combinée.
`Overall memory usage percentage to issue log info (Pourcentage d'utilisation de mémoire globale pour émettre des informations de journalisation)`	Spécifie le seuil auquel l'utilisation de mémoire système validée globale est journalisée. La mémoire système validée est la mémoire allouée par des processus et pour laquelle le système d'exploitation a validé la mémoire physique ou un emplacement de page dans le fichier d'échange.
`Process CPU usage percentage to issue log info (Pourcentage d'utilisation du CPU de processus pour émettre des informations de journalisation)`	Spécifie le seuil auquel l'utilisation de CPU d'un processus individuel est journalisée.
`Process memory usage percentage to issue log info (Pourcentage d'utilisation de mémoire de processus pour émettre des informations de journalisation)`	Spécifie le seuil auquel l'utilisation de mémoire d'un processus individuel est journalisée.
`Process to check, comma separated name list allowing wild cards and exclusion (Processus pour vérifier une liste de noms séparés par des virgules autorisant les caractères génériques et l'exclusion)`	Spécifie une liste séparée par des virgules de requêtes qui correspondent au nom d'un ou plusieurs processus à examiner. Vous pouvez filtrer la liste en utilisant des caractères génériques pour chaque requête. ■ Un astérisque (*) correspond à zéro caractère ou plus. ■ Un point d'interrogation (?) correspond exactement à un caractère. ■ Un point d'exclamation (!) au début d'une requête exclut tous les résultats produits par cette requête. Par exemple, la requête suivante sélectionne tous les processus commençant par **`ws`** et exclut tous les processus se terminant par **`sys`** : **`'!*sys,ws*'`**

REMARQUE Les paramètres d'alarme de performance ne s'appliquent qu'à des systèmes View Connection Server et View Agent. Ils ne s'appliquent pas à des systèmes View Client.

paramètres généraux

Tableau 8-33 décrit les paramètres généraux dans le fichier de modèle d'administration pour la configuration commune de View.

Tableau 8-33. Modèle de configuration commune de View : paramètres généraux

Paramètre	Propriétés
`Disk threshold for log and events in Megabytes (Seuil de disque pour les journaux et les événements en mégaoctets)`	Spécifie le seuil minimum d'espace disque restant pour les journaux et les événements. Si aucune valeur n'est spécifiée, la valeur par défaut est de 200. Lorsque la valeur spécifiée est atteinte, la journalisation des événements s'arrête.
`Enable extended logging (Activer la journalisation étendue)`	Détermine si les événements de suivi et de débogage sont inclus dans les fichiers journaux.

Paramètres de modèle d'administration pour les variables de session PCoIP de View

Le fichier de modèle d'administration pour les variables de session PCoIP de View (`pcoip.adm`) contient des paramètres de stratégie liés au protocole d'affichage PCoIP. Vous pouvez configurer des paramètres sur des valeurs par défaut, qui peuvent être remplacées par un administrateur, ou vous pouvez configurer des paramètres sur des valeurs ne pouvant pas être remplacées.

Le fichier de modèle d'administration pour les variables de session PCoIP de View contient deux sous-catégories :

Valeurs par défaut remplaçables par l'administrateur	Spécifie les valeurs par défaut des variables de session PCoIP. Ces paramètres peuvent être remplacés par un administrateur. Ces paramètres inscrivent des valeurs de clé de Registre sur `HKLM\Software\Policies\Teradici\PCoIP\pcoip_admin_defaults`.
Paramètres non remplaçables par l'administrateur	Contient les mêmes paramètres que Valeurs par défaut remplaçables par l'administrateur, mais ces paramètres ne peuvent pas être remplacés par un administrateur. Ces paramètres inscrivent des valeurs de clé de Registre sur `HKLM\Software\Policies\Teradici\PCoIP\pcoip_admin`.

Le modèle ne contient que des paramètres Configuration d'ordinateur.

Clés de Registre non liées à des stratégies

Si un paramètre de machine locale doit être appliqué et ne peut pas être placé sous `HKLM\Software\Policies\Teradici`, des paramètres de machine locale peuvent être placés dans des clés de Registre dans `HKLM\Software\Teradici`. Les mêmes clés de Registre peuvent être placées dans `HKLM\Software\Teradici` comme dans `HKLM\Software\Policies\Teradici`. Si la même clé de Registre est présente dans les deux emplacements, le paramètre dans `HKLM\Software\Policies\Teradici` remplace la valeur de machine locale.

- Variables de la session générale PCoIP de View page 239

  Le fichier de modèle d'administration pour les variables de session PCoIP de View contient des paramètres de stratégie de groupe qui configurent des caractéristiques de session générale telles que la qualité d'image PCoIP, les périphériques USB et les ports réseau.

- Variables de bande passante de la session PCoIP de View page 245

  Le fichier de modèle d'administration pour les variables de session PCoIP de View contient des paramètres de stratégie de groupe qui configurent des caractéristiques de bande passante de la session PCoIP.

- Variables de la session PCoIP de View pour le clavier page 248

  Le fichier de modèle d'administration pour les variables de session PCoIP de View contient des paramètres de stratégie de groupe qui configurent des caractéristiques de session PCoIP affectant l'utilisation du clavier.

- Fonction de développement sans perte PCoIP de View page 249

  Le protocole d'affichage PCoIP utilise une approche de codage appelée développement progressif, qui permet de fournir une expérience utilisateur globale optimale même dans des conditions de réseau contraintes.

Variables de la session générale PCoIP de View

Le fichier de modèle d'administration pour les variables de session PCoIP de View contient des paramètres de stratégie de groupe qui configurent des caractéristiques de session générale telles que la qualité d'image PCoIP, les périphériques USB et les ports réseau.

Tableau 8-34. Variables de la session générale PCoIP de View

Paramètre	Description
`Configurer la redirection du presse-papier`	Détermine la direction dans laquelle la redirection du presse-papier est autorisée. Vous pouvez sélectionner l'une de ces valeurs : ■ **[Activé uniquement du client au serveur]** (C'est-à-dire autoriser l'opération copier/coller uniquement depuis le système client vers le poste de travail View.) ■ **[Désactivé dans les deux directions]** ■ **[Activé dans les deux directions]** ■ **[Activé uniquement du serveur au client]** (C'est-à-dire autoriser l'opération copier/coller uniquement depuis le poste de travail View vers le système client.) La redirection du presse-papier est implémentée sous forme de canal virtuel. Si des canaux virtuels sont désactivés, la redirection du presse-papier ne fonctionne pas. Ce paramètre ne s'applique qu'à View Agent. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, la valeur par défaut est **[Activé uniquement du client au serveur]** .
`Configurer la règle de taille de cache d'images client PCoIP`	Contrôle la taille du cache d'images client PCoIP. Le client utilise une mise en cache d'images pour stocker des parties de l'affichage qui ont été précédemment transmises. La mise en cache d'images réduit la quantité de données qui sont retransmises. Ce paramètre ne s'applique qu'à des clients Windows et Linux lorsque View Client, View Agent et Serveur de connexion View sont la version View 5.0 ou supérieure. Lorsque ce paramètre n'est pas configuré ou qu'il est désactivé, PCoIP utilise une taille de cache d'images client par défaut de 250 Mo. Lorsque vous activez ce paramètre, vous pouvez configurer une taille de cache d'images client comprise entre 50 Mo minimum et 300 Mo maximum. La valeur par défaut est 250 Mo.
`Configurer le niveau de détails du journal des événements PCoIP`	Définit le niveau de détails du journal des événements PCoIP. Les valeurs sont comprises entre 0 (le moins de détails) et 3 (le plus de détails). Lorsque ce paramètre est activé, vous pouvez définir le niveau de détail entre 0 et 3. Lorsque le paramètre n'est pas configuré ou désactivé, le niveau de détail du journal des événements par défaut est 2. Lorsque ce paramètre est modifié lors d'une session PCoIP active, le nouveau paramètre prend effet immédiatement.

Tableau 8-34. Variables de la session générale PCoIP de View (suite)

Paramètre	Description
`Configurer des niveaux de qualité d'image PCoIP`	Contrôle comment PCoIP rend les images lors de périodes de surcharge du réseau. Les valeurs **[Qualité d'image minimale]**, **[Qualité d'image initiale maximale]** et **[Fréquence d'image maximale]** interagissent pour contrôler précisément des environnements contraints en termes de bande passante réseau. Utilisez la valeur **[Qualité d'image minimale]** pour équilibrer la qualité d'image et la fréquence d'image lorsque la bande passante est limitée. Vous pouvez spécifier une valeur comprise entre 30 et 100. La valeur par défaut est 50. Une valeur inférieure permet d'utiliser des fréquences d'image élevées, mais avec un affichage d'une qualité potentiellement inférieure. Une valeur supérieure fournit une qualité d'image supérieure, mais avec des fréquences d'image potentiellement inférieures lorsque la bande passante réseau est contrainte. Lorsque la bande passante réseau n'est pas contrainte, PCoIP conserve la qualité maximale quelle que soit cette valeur. Utilisez la valeur **[Qualité d'image initiale maximale]** pour réduire les pics de bande passante réseau requis par PCoIP en limitant la qualité initiale des régions modifiées de l'image affichée. Vous pouvez spécifier une valeur comprise entre 30 et 100. La valeur par défaut est 90. Une valeur inférieure réduit la qualité d'image des modifications de contenu et diminue les exigences de bande passante maximale. Une valeur supérieure augmente la qualité d'image des modifications de contenu et augmente les exigences de bande passante maximale. Les régions non modifiées de l'image entraînent progressivement une qualité sans perte (parfaite) quelle que soit cette valeur. Une valeur de 90 ou moins permet d'utiliser au mieux la bande passante disponible. La valeur **[Qualité d'image minimale]** ne peut pas dépasser la valeur **[Qualité d'image initiale maximale]**. Utilisez la valeur **[Fréquence d'image maximale]** pour gérer la bande passante moyenne consommée par utilisateur en limitant le nombre d'actualisations d'écran par seconde. Vous pouvez spécifier une valeur comprise entre 1 et 120 images par seconde. La valeur par défaut est 30. Une valeur supérieure peut utiliser plus de bande passante mais fournit moins de gigue, ce qui permet des transitions plus homogènes entre les images, comme dans une vidéo. Une valeur inférieure utilise moins de bande passante mais entraîne plus de gigue. Ces valeurs de qualité d'image ne s'appliquent qu'à l'hôte léger et n'ont aucun effet sur un client léger. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, les valeurs par défaut sont utilisées.
`Configurer des algorithmes de cryptage de la session PCoIP`	Contrôle les algorithmes de cryptage annoncés par le point de terminaison PCoIP lors de la négociation de session. Cocher l'une des cases désactive l'algorithme de cryptage associé. Vous devez activer au moins un algorithme. Par défaut, les deux algorithmes Salsa20-256round12 et AES-128-GCM sont disponibles pour la négociation par ce point de terminaison. Ce paramètre s'applique à la fois au serveur et au client. Les points de terminaison négocient l'algorithme de cryptage de session réel qui est utilisé. Si le mode approuvé FIPS140-2 est activé, la valeur **[Désactiver le cryptage AES-128-GCM]** est toujours remplacée pour que le cryptage AES-128-GCM soit activé. Si ce paramètre est désactivé ou qu'il n'est pas configuré, les deux algorithmes Salsa20-256round12 et AES-128-GCM sont disponibles pour la négociation par ce point de terminaison.

Tableau 8-34. Variables de la session générale PCoIP de View (suite)

Paramètre	Description
`Configurer des règles de périphériques USB autorisés et interdits pour PCoIP`	Spécifie les périphériques USB autorisés et interdits pour les sessions PCoIP qui utilisent un client zéro exécutant le microprogramme Teradici. Les périphériques USB utilisés dans des sessions PCoIP doivent apparaître dans la table d'autorisation USB. Les périphériques USB qui apparaissent dans la table d'interdiction USB ne peuvent pas être utilisés dans des sessions PCoIP. Vous pouvez définir un maximum de 10 règles d'autorisation USB et un maximum de 10 règles d'interdiction USB. Séparez les valeurs avec le caractère de barre verticale (|). Chaque règle peut être une combinaison d'un ID de fournisseur (VID) et d'un ID de produit (PID), ou une règle peut décrire une classe de périphériques USB. Une règle de classe peut autoriser ou interdire une classe de périphériques entière, une seule sous-classe ou un protocole dans une sous-classe. Le format d'une combinaison de règle VID/PID est **`1xxxxyyyy`**, où **`xxxx`** est le VID au format hexadécimal et **`yyyy`** le PID au format hexadécimal. Par exemple, la règle pour autoriser ou bloquer un périphérique avec le VID **`0x1a2b`** et le PID **`0x3c4d`** est **`11a2b3c4d`**. Pour des règles de classe, utilisez l'un des formats suivants : **Autoriser tous les périphériques USB** — Format : **`23XXXXXX`** ; Exemple : **`23XXXXXX`** **Autoriser tous les périphériques USB avec un ID de classe spécifique** — Format : **`22`*`class`*`XXXX`** ; Exemple : **`22aaXXXX`** **Autoriser une sous-classe spécifique** — Format : **`21`*`class-subclass`*`XX`** ; Exemple : **`21aabbXX`** **Autoriser un protocole spécifique** — Format : **`20`*`class-subclass-protocol`** ; Exemple : **`20aabbcc`** Par exemple, la chaîne d'autorisation USB pour autoriser les périphériques HID USB (souris et clavier) (ID de classe 0x03) et les webcams (ID de classe 0x0e) est **`2203XXXX|220eXXXX`**. La chaîne d'interdiction USB pour interdire les périphériques de stockage de masse USB (ID de classe 0x08) est **`2208XXXX`**. Une chaîne d'autorisation USB vide signifie qu'aucun périphérique USB n'est autorisé. Une chaîne d'interdiction USB vide signifie qu'aucun périphérique USB n'est interdit. Ce paramètre ne s'applique qu'à View Agent et uniquement quand le poste de travail View Agent se trouve dans une session avec un client zéro qui exécute le microprogramme Teradici. L'utilisation de périphérique est négociée entre les points de terminaison. Par défaut, tous les périphériques sont autorisés et aucun n'est interdit.

Tableau 8-34. Variables de la session générale PCoIP de View (suite)

Paramètre	Description
`Configurer des canaux virtuels PCoIP`	Spécifie les canaux virtuels qui peuvent et ne peuvent pas fonctionner sur des sessions PCoIP. Ce paramètre détermine également s'il est nécessaire de désactiver le traitement du presse-papier sur l'hôte PCoIP. Les canaux virtuels utilisés dans des sessions PCoIP doivent apparaître dans la liste d'autorisation des canaux virtuels. Les canaux virtuels qui apparaissent dans la liste des canaux virtuels interdits ne peuvent pas être utilisés dans des sessions PCoIP. Vous pouvez spécifier un maximum de 15 canaux virtuels à utiliser dans des sessions PCoIP. Séparez les noms de canal avec le caractère de barre verticale (`|`). Par exemple, la chaîne d'autorisation des canaux virtuels pour autoriser les canaux virtuels mksvchan et vdp_rdpvcbridge est **`mksvchan|vdp_vdpvcbridge`**. Si un nom de canal contient le caractère de barre verticale ou de barre oblique inverse (`\`), insérez un caractère de barre oblique inverse avant ce caractère. Par exemple, saisissez le nom de canal awk|ward\channel comme suit : **`awk\\|ward\\channel`**. Lorsque la liste des canaux virtuels autorisés est vide, tous les canaux virtuels sont interdits. Lorsque la liste des canaux virtuels interdits est vide, tous les canaux virtuels sont autorisés. Le paramètre des canaux virtuels s'applique à la fois au serveur et au client. Les canaux virtuels doivent être activés à la fois sur le serveur et le client pour pouvoir être utilisés. Le paramètre des canaux virtuels fournit une case séparée qui vous permet de désactiver le traitement du presse-papier à distance sur l'hôte PCoIP. Cette valeur ne s'applique qu'au serveur. Par défaut, tous les canaux virtuels sont activés, notamment le traitement du presse-papier.
`Configurer le port UDP PCoIP du client`	Spécifie le port client UDP utilisé par les clients PCoIP logiciels. La valeur du port UDP spécifie le port UDP de base à utiliser. La valeur de plage du port UDP détermine le nombre de ports supplémentaires à essayer si le port de base n'est pas disponible. La plage s'étend du port de base à la somme du port de base et de la plage du port. Par exemple, si le port de base est 50002 et que la plage du port est 64, la plage s'étend de 50002 à 50066. Ce paramètre ne s'applique qu'au client. Par défaut, le port de base est 50002 et la plage du port est 64.

Tableau 8-34. Variables de la session générale PCoIP de View (suite)

Paramètre	Description
`Configurer l'en-tête de transport PCoIP`	Configure l'en-tête de transport PCoIP et définit la priorité de la session de transport. L'en-tête de transport PCoIP est un en-tête 32 bits ajouté à tous les paquets UDP PCoIP (uniquement si l'en-tête de transport est activé et pris en charge des deux côtés). L'en-tête de transport PCoIP permet aux périphériques réseau de prendre de meilleures décisions concernant la hiérarchisation/qualité de service lors du traitement de la surcharge du réseau. L'en-tête de transport est activé par défaut. La priorité de session de transport détermine la priorité de session PCoIP signalée dans l'en-tête de transport PCoIP. Les périphériques réseau prennent de meilleures décisions concernant la hiérarchisation/qualité de service en fonction de la priorité de session de transport spécifiée. Lorsque le paramètre `Configurer l'en-tête de transport PCoIP` est activé, les priorités de session de transport suivantes sont disponibles : ■ **[Élevée]** ■ **[Moyenne]** (valeur par défaut) ■ **[Faible]** ■ **[Non défini]** La valeur de priorité de session de transport est négociée par l'agent et le client PCoIP. Si l'agent PCoIP spécifie une valeur de priorité de session de transport, la session utilise la priorité de session spécifiée par l'agent. Si seul le client a spécifié une priorité de session de transport, la session utilise la priorité de session spécifiée par le client. Si ni l'agent ni le client n'a spécifié une priorité de session de transport, ou si **[Priorité non définie]** est spécifié, la session utilise la valeur par défaut, la priorité **[Moyenne]** .
`Configurer le port TCP auquel l'hôte PCoIP se lie et qu'il écoute`	Spécifie le port serveur TCP lié par des hôtes PCoIP logiciels. La valeur du port TCP spécifie le port TCP de base auquel le serveur tente de se lier. La valeur de plage du port TCP détermine le nombre de ports supplémentaires à essayer si le port de base n'est pas disponible. La plage du port doit être comprise entre 0 et 10. La plage s'étend du port de base à la somme du port de base et de la plage du port. Par exemple, si le port de base est 4172 et que la plage du port est 10, la plage s'étend de 4172 à 4182. Ce paramètre ne s'applique qu'à View Agent. Par défaut, le port TCP de base est 4172 pour View 4.5 et supérieur et 50002 pour View 4.0.*x* et antérieur. Par défaut, la plage de port est 1.
`Configurer le port UDP auquel l'hôte PCoIP se lie et qu'il écoute`	Spécifie le port serveur UDP lié par des hôtes PCoIP logiciels. La valeur du port UDP spécifie le port UDP de base auquel le serveur tente de se lier. La valeur de plage du port UDP détermine le nombre de ports supplémentaires à essayer si le port de base n'est pas disponible. La plage du port doit être comprise entre 0 et 10. La plage s'étend du port de base à la somme du port de base et de la plage du port. Par exemple, si le port de base est 4172 et que la plage du port est 10, la plage s'étend de 4172 à 4182. Ce paramètre ne s'applique qu'à View Agent. Par défaut, le port TCP de base est 4172 pour View 4.5 et supérieur et 50002 pour View 4.0.*x* et antérieur. Par défaut, la plage de port est 10.

Tableau 8-34. Variables de la session générale PCoIP de View (suite)

Paramètre	Description
`Autoriser l'accès à une session PCoIP depuis une console vSphere`	Détermine s'il est nécessaire d'autoriser une console vSphere Client à afficher une session PCoIP active et à envoyer l'entrée au poste de travail. Par défaut, lorsqu'un client est attaché via PCoIP, l'écran de la console vSphere Client est vide et la console ne peut pas envoyer l'entrée. Le paramètre par défaut garantit qu'un utilisateur malveillant ne peut pas voir le poste de travail de l'utilisateur ou fournir d'entrées sur l'hôte localement lorsqu'une session distante PCoIP est active. Ce paramètre ne s'applique qu'à View Agent. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, l'accès à la console n'est pas autorisé. Lorsque ce paramètre est activé, la console affiche la session PCoIP et l'entrée de console est autorisée. Lorsque ce paramètre est activé, la console peut afficher une session PCoIP exécutée sur un système Windows 7 uniquement lorsque la machine virtuelle Windows 7 est de version matérielle v8. La version matérielle v8 n'est disponible que sur ESX 5.0 et supérieur. A contrario, l'entrée de console sur un système Windows 7 est autorisée quelle que soit la version matérielle de la machine virtuelle. Sur un système Windows XP ou Windows Vista, la console peut afficher une session PCoIP quelle que soit la version matérielle de la machine virtuelle.
`Activer le mode d'opération approuvé FIPS 140-2`	Détermine s'il est nécessaire d'utiliser uniquement des algorithmes et des protocoles cryptographiques approuvés FIPS 140-2 pour établir une connexion PCoIP à distance. Activer ce paramètre remplace la désactivation du cryptage AES128-GCM. Ce paramètre s'applique à la fois au serveur et au client. Vous pouvez configurer un ou les deux points de terminaison pour qu'ils fonctionnent en mode FIPS. La configuration d'un seul point de terminaison pour qu'il fonctionne en mode FIPS limite les algorithmes de cryptage disponibles pour la négociation de session. Le mode FIPS est disponible pour View 4.5 et supérieur. Pour View 4.0.*x* et antérieur, le mode FIPS n'est pas disponible, et la configuration de ce paramètre n'a aucun effet. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, le mode FIPS n'est pas utilisé.
`Activer/désactiver le son dans la session PCoIP`	Détermine si le son est activé dans des sessions PCoIP. Le son doit être activé sur les deux points de terminaison. Lorsque ce paramètre est activé, le son PCoIP est autorisé. Lorsqu'il est désactivé, le son PCoIP est désactivé. Lorsque ce paramètre n'est pas configuré, le son est activé par défaut.
`Activer/désactiver le bruit microphonique et le filtre de tension de décalage continue dans une session PCoIP`	Détermine s'il est nécessaire d'activer le bruit microphonique et le filtre de tension de décalage continue pour l'entrée de microphone lors de sessions PCoIP. Ce paramètre ne s'applique qu'à View Agent et au pilote audio Teradici. Lorsque ce paramètre n'est pas configuré, le pilote audio Teradici utilise le bruit microphonique et le filtre de tension de décalage continue par défaut.
`Activer la synchronisation de la langue d'entrée par défaut de l'utilisateur PCoIP`	Détermine si la langue d'entrée par défaut pour l'utilisateur dans la session PCoIP est synchronisée avec la langue d'entrée par défaut du point de terminaison du client PCoIP. Lorsque ce paramètre est activé, la synchronisation est autorisée. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, la synchronisation est interdite. Ce paramètre ne s'applique qu'à View Agent.

Variables de bande passante de la session PCoIP de View

Le fichier de modèle d'administration pour les variables de session PCoIP de View contient des paramètres de stratégie de groupe qui configurent des caractéristiques de bande passante de la session PCoIP.

Tableau 8-35. Variables de bande passante de la session PCoIP de View

Paramètre	Description
`Configure the maximum PCoIP session bandwidth`	Spécifie la bande passante maximale, en kilobits par seconde, dans une session PCoIP. La bande passante inclut la création d'images, le son, le canal virtuel, USB et le trafic PCoIP de contrôle. Définissez cette valeur sur la capacité globale du lien auquel votre point de terminaison est connecté. Par exemple, pour un client qui se connecte avec une connexion Internet de 4 Mbit/s, définissez cette valeur sur 4 Mbits soit 10 % de moins que cette valeur. Définir cette valeur empêche le serveur de transmettre un taux supérieur à la capacité de lien, qui pourrait entraîner une perte de paquets excessive et une mauvaise expérience utilisateur. Cette valeur est symétrique. Elle force le client et le serveur à utiliser la plus faible des deux valeurs qui sont définies du côté client et serveur. Par exemple, définir une bande passante maximale de 4 Mbit/s force le serveur à transmettre à un taux plus faible, même si le paramètre est configuré sur le client. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré sur un point de terminaison, le point de terminaison n'impose aucune contrainte de bande passante. Lorsque ce paramètre est configuré, le paramètre est utilisé comme la contrainte de bande passante maximale du point de terminaison en kilobits par seconde. La valeur par défaut lorsque ce paramètre n'est pas configuré est de 90 000 kilobits par seconde. Ce paramètre s'applique à View Agent et au client. Si les deux points de terminaison ont des paramètres différents, la valeur la plus faible est utilisée.
`Configure the PCoIP session bandwidth floor (Configurer la valeur plancher de la bande passante de la session PCoIP)`	Spécifie une limite inférieure, en kilobits par seconde, pour la bande passante réservée par la session PCoIP. Ce paramètre configure le taux de transmission de bande passante minimum attendu pour le point de terminaison. Lorsque vous utilisez ce paramètre pour réserver de la bande passante pour un point de terminaison, l'utilisateur n'a pas à attendre que la bande passante soit disponible, ce qui améliore la réactivité de la session. Assurez-vous que vous ne sursouscrivez pas la bande passante totale réservée pour tous les points de terminaison. Assurez-vous que la somme des valeurs plancher de la bande passante pour toutes les connexions dans votre configuration ne dépasse pas la capacité du réseau. La valeur par défaut est 0, ce qui signifie qu'aucune bande passante minimale n'est réservée. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, aucune bande passante minimale n'est réservée. Ce paramètre s'applique à View Agent et au client, mais il n'affecte que le point de terminaison sur lequel il est configuré.

Tableau 8-35. Variables de bande passante de la session PCoIP de View (suite)

Paramètre	Description
`Configure the PCoIP session MTU`	Spécifie la taille de l'unité de transmission maximale (MTU) pour les paquets UDP d'une session PCoIP. La taille de la MTU inclut les en-têtes de paquet IP et UDP. Le protocole TCP utilise le mécanisme de découverte MTU standard pour définir la MTU et n'est pas affecté par ce paramètre. La taille de la MTU maximale est de 1 500 octets. La taille de la MTU minimale est de 500 octets. La valeur par défaut est de 1 300 octets. En général, vous n'avez pas à modifier la taille de la MTU. Modifiez cette valeur si vous avez une configuration de réseau inhabituelle qui provoque une fragmentation de paquets PCoIP. Ce paramètre s'applique à View Agent et au client. Si les deux points de terminaison ont des paramètres de taille de MTU différents, la valeur la plus faible est utilisée. Si ce paramètre est désactivé ou qu'il n'est pas configuré, le client utilise la valeur par défaut dans la négociation avec View Agent.

Tableau 8-35. Variables de bande passante de la session PCoIP de View (suite)

Paramètre	Description
`Configure the PCoIP session audio bandwidth limit`	Spécifie la bande passante maximale pouvant être utilisée pour le son (lecture audio) dans une session PCoIP. Le traitement audio surveille la bande passante utilisée pour le son. Le traitement sélectionne l'algorithme de compression audio qui fournit le meilleur son possible, en fonction de l'utilisation actuelle de la bande passante. Si une limite de bande passante est définie, le traitement réduit la qualité en modifiant la sélection de l'algorithme de compression jusqu'à ce que la limite de bande passante soit atteinte. S'il n'est pas possible d'atteindre un son de qualité minimale dans la limite de bande passante spécifiée, le son est désactivé. Pour un son stéréo non compressé de haute qualité, définissez cette valeur sur plus de 1 600 kbit/s. Une valeur de 450 kbit/s et plus permet d'obtenir un son stéréo compressé de haute qualité. Une valeur comprise entre 50 kbit/s et 450 kbit/s donne un son dont la qualité va de celle d'une radio FM à celle d'un appel téléphonique. Une valeur inférieure à 50 kbit/s peut entraîner une lecture sans son. Ce paramètre ne s'applique qu'à View Agent. Vous devez activer le son sur les deux points de terminaison avant que ce paramètre ne prenne effet. En outre, ce paramètre n'a pas d'effet sur l'audio USB. Si ce paramètre est désactivé ou qu'il n'est pas configuré, une limite de bande passante audio par défaut de 500 kilobits par seconde est configurée pour contraindre l'algorithme de compression audio sélectionné. Si le paramètre est configuré, la valeur est mesurée en kilobits par seconde, avec une limite de bande passante audio par défaut de 500 kilobits par seconde. Ce paramètre s'applique à View 4.6 et supérieur. Il n'a aucun effet sur les versions antérieures de View.
`Turn off Build-to-Lossless feature`	Spécifie s'il est nécessaire de désactiver la fonction de développement sans perte du protocole PCoIP, qui est activée par défaut. Si vous activez ce paramètre, la fonction de développement sans perte est désactivée. Les images et autre contenu du poste de travail ne sont jamais développés vers un état sans perte. Dans des environnements de réseau avec une bande passante contrainte, la désactivation de la fonction de développement sans perte peut permettre d'économiser de la bande passante. La désactivation de cette fonction n'est pas recommandée dans les environnements qui requièrent que les images et le contenu de poste de travail soient développés vers un état sans perte. Pour activer ce paramètre, vous devez cliquer sur **[Enabled (Activé)]** et cochez la case suivante : **[I accept to turn off the Build-to-Lossless feature (J'accepte de désactiver la fonction de développement sans perte)]** . Cet accord indique que vous comprenez que les images et le contenu de poste de travail ne sont jamais développés vers un état sans perte. Pour plus d'informations sur la fonction de développement sans perte PCoIP, reportez-vous à la section « Fonction de développement sans perte PCoIP de View », page 249.

Variables de la session PCoIP de View pour le clavier

Le fichier de modèle d'administration pour les variables de session PCoIP de View contient des paramètres de stratégie de groupe qui configurent des caractéristiques de session PCoIP affectant l'utilisation du clavier.

Tableau 8-36. Variables de la session PCoIP de View pour le clavier

Paramètre	Description
`Disable sending CAD when users press Ctrl+Alt+Del`	Lorsque cette stratégie est activée, les utilisateurs doivent appuyer sur Ctrl +Alt+Inser au lieu de Ctrl+Alt+Suppr pour envoyer une séquence de touches de sécurité (SAS, Secure Attention Sequence) au poste de travail lors d'une session PCoIP. Vous voulez peut-être activer ce paramètre si des utilisateurs sont confus lorsqu'ils appuient sur Ctrl+Alt+Suppr pour verrouiller le point de terminaison du client et qu'une SAS est envoyée à l'hôte et au client. Ce paramètre ne s'applique qu'à View Agent et n'a aucun effet sur un client. Lorsque cette stratégie n'est pas configurée ou qu'elle est désactivée, les utilisateurs peuvent appuyer sur Ctrl+Alt+Suppr ou Ctrl+Alt+Inser pour envoyer une SAS au poste de travail.
`Enable Right SHIFT behavior when a PCoIP client is connected (Activer le comportement de la touche Maj droite lorsqu'un client PCoIP est connecté)`	Détermine si vous voulez activer la substitution de la touche Maj droite avec la touche Maj gauche, ce qui permet à la touche Maj droite de fonctionner correctement lors de l'utilisation de RDP via PCoIP. Ce paramètre peut être utilisé lorsque RDP est utilisé dans une session PCoIP. Ce paramètre ne s'applique qu'à View Agent et n'a aucun effet sur un client. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, la substitution n'est pas effectuée. Sur des postes de travail qui exécutent View Agent 4.6 et supérieur, la touche Maj droite fonctionne correctement lorsque RDP est utilisé dans une session PCoIP. Utilisez ce paramètre uniquement sur des postes de travail exécutant View Agent 4.5 et antérieur. Pour View Agent 4.6, ce paramètre est appliqué, mais il n'est pas nécessaire. Pour View Agent 5.0 et supérieur, ce paramètre n'est pas appliqué même lorsqu'il est configuré.

Tableau 8-36. Variables de la session PCoIP de View pour le clavier (suite)

Paramètre	Description
`Use alternate key for sending Secure Attention Sequence`	Spécifie une touche alternative, à la place de la touche Inser, pour l'envoi d'une séquence de touches de sécurité (SAS, Secure Attention Sequence). Vous pouvez utiliser ce paramètre pour conserver la séquence de touches Ctrl+Alt+Inser sur des machines virtuelles démarrées depuis un poste de travail View au cours d'une session PCoIP. Par exemple, un utilisateur peut démarrer un vSphere Client depuis un poste de travail PCoIP et ouvrir une console sur une machine virtuelle dans vCenter Server. Si la séquence Ctrl+Alt+Inser est utilisée dans le Système d'exploitation client sur la machine virtuelle vCenter Server, une SAS Ctrl+Alt+Suppr est envoyée à la machine virtuelle. Ce paramètre permet à la séquence Ctrl+Alt+*Alternate Key* d'envoyer une SAS Ctrl+Alt +Suppr au poste de travail PCoIP. Lorsque ce paramètre est activé, vous devez sélectionner une autre touche depuis un menu déroulant. Vous ne pouvez pas activer ce paramètre et laisser la valeur non spécifiée. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, la séquence de touches Ctrl+Alt+Inser est utilisée comme SAS. Ce paramètre ne s'applique qu'à View Agent et n'a aucun effet sur un client.
`Use enhanced keyboard on Windows client if available`	Détermine s'il est nécessaire de diriger des séquences clavier à restreindre au Système d'exploitation client dans des sessions de poste de travail PCoIP. Lorsque vous appuyez sur Ctrl+Alt+Suppr, Win+L, ou une autre séquence clavier, seul le système d'exploitation, plutôt que le client et l'hôte, agit sur la commande. Par exemple, appuyer sur Ctrl+Alt+Suppr ne verrouille pas le système hôte. Ce paramètre ne s'applique qu'aux hôtes Windows. Avant que le paramètre de clavier étendu puisse prendre effet, le pilote de filtre de clavier VMware, `vmkbd.sys`, doit être installé et configuré. Le pilote de filtre de clavier VMware est automatiquement installé et configuré sur des ordinateurs sur lesquels VMware Workstation, Player ou View Client with Local Mode sont installés. Vous pouvez utiliser ce paramètre uniquement lorsque View Client est exécuté par un membre du groupe de l'administrateur sur Windows XP ou est exécuté sous des privilèges élevés par **Run as administrator (Exécuter en tant qu'administrateur)** sous Windows Vista et supérieur. Ce paramètre permet au système hôte Windows de traiter la saisie au clavier par une autre méthode. Il traite la saisie au clavier brute dès que possible, en outrepassant le traitement de frappe Windows et les logiciels malveillants qui ne se trouvent pas déjà dans une couche inférieure. Utilisez le clavier virtuel étendu si la machine virtuelle peut être utilisée par une personne avec un clavier international ou un clavier avec des touches supplémentaires. Lorsque cette stratégie n'est pas configurée ou qu'elle est désactivée, la fonction de clavier étendu n'est pas utilisée.

Fonction de développement sans perte PCoIP de View

Le protocole d'affichage PCoIP utilise une approche de codage appelée développement progressif, qui permet de fournir une expérience utilisateur globale optimale même dans des conditions de réseau contraintes.

Le développement progressif fournit une image initiale hautement compressée, appelée image avec perte, qui est ensuite progressivement développée vers un état sans perte complet. Un état sans perte signifie que l'image apparaît avec la haute fidélité prévue.

Sur un réseau LAN, PCoIP affiche toujours le texte à l'aide de la compression sans perte. Si la bande passante par session disponible passe en dessous de 1 Mbit/s, PCoIP affiche initialement une image texte avec perte et développe rapidement l'image vers un état sans perte. Cette approche permet au poste de travail de rester réactif et d'afficher la meilleure image possible lorsque les conditions de réseau changent, ce qui offre aux utilisateurs une expérience optimale.

La fonction de développement sans perte fournit les caractéristiques suivantes :

- règle dynamiquement la qualité d'image ;
- réduit la qualité d'image sur les réseaux encombrés ;
- maintient la réactivité en réduisant la latence de mise à jour de l'écran ;
- reprend la qualité d'image maximale lorsque le réseau n'est plus encombré.

Le protocole PCoIP est assez efficace pour fournir la fonction de développement sans perte dans toutes les conditions, ce qui permet à cette fonction de rester activée par défaut.

Vous pouvez désactiver la fonction de développement sans perte en définissant le paramètre de stratégie de groupe `Turn off Build-to-Lossless feature`. Reportez-vous à la section « Variables de bande passante de la session PCoIP de View », page 245.

Configuration de l'impression basée sur l'emplacement

La fonction d'impression basée sur l'emplacement mappe les imprimantes physiquement proches des systèmes client vers des postes de travail View, ce qui permet aux utilisateurs d'imprimer sur leurs imprimantes locales et en réseau depuis leurs postes de travail View.

La fonction d'impression basée sur l'emplacement est disponible pour les systèmes client Windows et non Windows. L'impression basée sur l'emplacement permet aux services informatiques de mapper des postes de travail View vers l'imprimante la plus proche du périphérique client de point de terminaison. Par exemple, lorsqu'un médecin passe de chambre en chambre dans un hôpital, chaque fois qu'il imprime un document, le travail d'impression est envoyé à l'imprimante la plus proche. Pour utiliser cette fonction, il n'est pas nécessaire que les bons pilotes d'imprimante soient installés sur le poste de travail View.

Vous réglez l'impression basée sur l'emplacement en configurant le paramètre de stratégie de groupe Active Directory `AutoConnect Map Additional Printers for VMware View`, situé dans l'Éditeur d'objets de stratégie de groupe de Microsoft dans le dossier **[Software Settings (Paramètres du logiciel)]** sous **[Computer Configuration (Configuration ordinateur)]** .

Remarque `AutoConnect Map Additional Printers for VMware View` est une stratégie spécifique à l'ordinateur. Les stratégies spécifiques à l'ordinateur s'appliquent à tous les postes de travail View, quelle que soit la personne se connectant au poste de travail.

`AutoConnect Map Additional Printers for VMware View` est un tableau de traduction de noms. Vous utilisez chaque ligne du tableau pour identifier une imprimante spécifique et définir un ensemble de règles de traduction pour cette imprimante. Les règles de traduction déterminent si l'imprimante est mappée vers le poste de travail View pour un système client particulier.

Lorsqu'un utilisateur se connecte à un poste de travail View, View compare le système client avec les règles de traduction associées à chaque imprimante du tableau. Si le système client satisfait toutes les règles de traduction définies pour l'imprimante, ou si une imprimante n'a pas de règle de traduction associée, View mappe l'imprimante vers le poste de travail View au cours de la session de l'utilisateur.

Vous pouvez définir des règles de traduction basées sur l'adresse IP, le nom et l'adresse MAC du système client, et sur le nom et le groupe de l'utilisateur. Vous pouvez spécifier une règle de traduction, ou une combinaison de plusieurs règles de traduction, pour une imprimante spécifique.

Les informations utilisées pour mapper l'imprimante vers le poste de travail View sont stockées dans une entrée de registre sur le poste de travail View dans `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\thinprint\tpautoconnect`.

1 Enregistrer le fichier DLL de la stratégie de groupe de l'impression basée sur l'emplacement page 251

Avant de pouvoir configurer le paramètre de stratégie de groupe pour l'impression basée sur l'emplacement, vous devez enregistrer le fichier DLL `TPVMGPoACmap.dll`.

2 Configurer la stratégie de groupe de l'impression basée sur l'emplacement page 251

Pour régler l'impression basée sur l'emplacement, vous configurez le paramètre de stratégie de groupe `AutoConnect Map Additional Printers for VMware View`. Le paramètre de stratégie de groupe est un tableau de traduction de noms qui mappe des imprimantes vers des postes de travail View.

Enregistrer le fichier DLL de la stratégie de groupe de l'impression basée sur l'emplacement

Avant de pouvoir configurer le paramètre de stratégie de groupe pour l'impression basée sur l'emplacement, vous devez enregistrer le fichier DLL `TPVMGPoACmap.dll`.

View fournit des versions 32 bits et 64 bits de `TPVMGPoACmap.dll` dans le répertoire *`install_directory`*`\VMware\VMware View\Server\extras\GroupPolicyFiles\ThinPrint` sur votre hôte de View Connection Server.

Procédure

1 Copiez la version appropriée de `TPVMGPoACmap.dll` sur votre serveur Active Directory ou sur l'ordinateur de domaine que vous utilisez pour configurer des stratégies de groupe.

2 Utilisez l'utilitaire `regsvr32` pour enregistrer le fichier `TPVMGPoACmap.dll`.

Par exemple : `regsvr32 "C:\TPVMGPoACmap.dll"`

Suivant

Configurez le paramètre de stratégie de groupe pour l'impression basée sur l'emplacement.

Configurer la stratégie de groupe de l'impression basée sur l'emplacement

Pour régler l'impression basée sur l'emplacement, vous configurez le paramètre de stratégie de groupe `AutoConnect Map Additional Printers for VMware View`. Le paramètre de stratégie de groupe est un tableau de traduction de noms qui mappe des imprimantes vers des postes de travail View.

Prérequis

- Vérifiez que les composants logiciels enfichables Microsoft MMC et que l'Éditeur d'objets de stratégie de groupe sont disponibles sur votre serveur Active Directory ou sur l'ordinateur de domaine que vous utilisez pour configurer des stratégies de groupe.
- Enregistrez le fichier DLL `TPVMGPoACmap.dll` sur votre serveur Active Directory ou sur l'ordinateur de domaine que vous utilisez pour configurer des stratégies de groupe. Reportez-vous à la section « Enregistrer le fichier DLL de la stratégie de groupe de l'impression basée sur l'emplacement », page 251.
- Familiarisez-vous avec la syntaxe du paramètre de stratégie de groupe `AutoConnect Map Additional Printers for VMware View`. Reportez-vous à la section « Syntaxe de paramètre de stratégie de groupe de l'impression basée sur l'emplacement », page 252.
- Créez un GPO pour le paramètre de stratégie de groupe basé sur l'emplacement et liez-le à l'UO qui contient vos postes de travail View. Pour voir un exemple de création de GPO pour des stratégies de groupe View, reportez-vous à la section « Créer des GPO pour les stratégies de groupe View », page 256.

- Comme les travaux d'impression sont envoyés directement du poste de travail View vers l'imprimante, vérifiez que les pilotes d'imprimante requis sont installés sur vos postes de travail.

Procédure

1 Sur le serveur Active Directory, modifiez le GPO.

Version AD	Chemin de navigation
Windows 2003	a Sélectionnez **[Start (Démarrer)] > [All Programs (Tous les programmes)] > [Administrative Tools (Outils d'administration)] > [Active Directory Users and Computers (Utilisateurs et ordinateurs Active Directory)]** . b Cliquez avec le bouton droit sur l'UO qui contient vos postes de travail View et sélectionnez **[Properties (Propriétés)]** . c Sous l'onglet **[Group Policy (Stratégie de groupe)]** , cliquez sur **[Open (Ouvrir)]** pour ouvrir le plug-in Group Policy Management (Gestion de stratégie de groupe). d Dans le volet de droite, cliquez avec le bouton droit sur le GPO que vous avez créé pour le paramètre de stratégie de groupe d'impression basée sur l'emplacement et sélectionnez **[Edit (Modifier)]** .
Windows 2008	a Sélectionnez **[Start (Démarrer)] > [Administrative Tools (Outils d'administration)] > [Group Policy Management (Gestion de stratégie de groupe)]** . b Développez votre domaine, cliquez avec le bouton droit sur l'objet GPO que vous avez créé pour le paramètre de stratégie de groupe d'impression en fonction de l'emplacement et sélectionnez **[Edit (Modifier)]** .

La fenêtre Group Policy Object Editor (Éditeur d'objets de stratégie de groupe) apparaît.

2 Développez **[Computer Configuration (Configuration ordinateur)]** , ouvrez le dossier **[Software Settings (Paramètres du logiciel)]** et sélectionnez **[AutoConnect Map Additional Printers for VMware View (Imprimantes supplémentaires de mappage de connexion automatique pour VMware View)]** .

3 Dans le volet Policy (Stratégie), double-cliquez sur **[Configure AutoConnect Map Additional Printers (Configurer des imprimantes supplémentaires de mappage de connexion automatique)]** .

La fenêtre AutoConnect Map Additional Printers for VMware View (Imprimantes supplémentaires de mappage de connexion automatique pour VMware View) apparaît.

4 Sélectionnez **[Enabled (Activé)]** pour activer le paramètre de stratégie de groupe.

Les titres et les boutons du tableau de traduction apparaissent dans la fenêtre de stratégie de groupe.

IMPORTANT Cliquer sur **[Disabled (Désactivé)]** supprime toutes les entrées du tableau. Par précaution, enregistrez votre configuration pour pouvoir l'importer ultérieurement.

5 Ajoutez les imprimantes que vous voulez mapper vers des postes de travail View et définissez leurs règles de traduction associées.

6 Cliquez sur **[OK]** pour enregistrer vos modifications.

Syntaxe de paramètre de stratégie de groupe de l'impression basée sur l'emplacement

Vous utilisez le paramètre de stratégie de groupe `AutoConnect Map Additional Printers for VMware View` pour mapper des imprimantes vers des postes de travail View.

`AutoConnect Map Additional Printers for VMware View` est un tableau de traduction de noms qui identifie des imprimantes et définit des règles de traduction associées. Tableau 8-37 décrit la syntaxe du tableau de traduction.

Tableau 8-37. Colonnes et valeurs contenues dans le tableau de traduction

Colonne	Description
IP Range	Règle de traduction spécifiant une plage d'adresses IP pour des systèmes client. Pour spécifier des adresses IP dans une plage spécifique, utilisez la notation suivante : ***ip_address-ip_address*** Par exemple : **10.112.116.0-10.112.119.255** Pour spécifier toutes les adresses IP dans un sous-réseau spécifique, utilisez la notation suivante : *ip_address/subnet_mask_bits* Par exemple : **10.112.4.0/22** Cette notation spécifie les adresses IPv4 utilisables de 10.112.4.1 à 10.112.7.254. Saisissez un astérisque pour inclure toutes les adresses IP.
Client Name	Règle de traduction spécifiant un nom d'ordinateur. Par exemple : **Ordinateur de Marie** Saisissez un astérisque pour inclure tous les noms d'ordinateur.
Mac Address	Règle de traduction spécifiant une adresse MAC. Dans l'éditeur de GPO, vous devez voir le même format que celui utilisé par le système client. Par exemple : ■ Les clients Windows utilisent des traits d'union : **01-23-45-67-89-ab** ■ Les clients Linux utilisent des deux-points : **01:23:45:67:89:ab** Saisissez un astérisque pour inclure toutes les adresses MAC.
User/Group	Règle de traduction spécifiant un nom d'utilisateur ou de groupe. Par exemple : **jdoe** Saisissez un astérisque pour inclure tous les noms d'utilisateur ou de groupe.
Printer Name	Nom de l'imprimante quand elle est mappée vers le poste de travail View. Par exemple : **PRINTER-2-CLR** Le nom mappé n'a pas à correspondre au nom de l'imprimante sur le système client.
Printer Driver	Nom du pilote qu'utilise l'imprimante. Par exemple : **HP Color LaserJet 4700 PS** IMPORTANT Comme les travaux d'impression sont envoyés directement du poste de travail vers l'imprimante, le pilote d'imprimante doit être installé sur le poste de travail.
IP Port/ThinPrint Port	Pour les imprimantes en réseau, adresses IP de l'imprimante avec le préfixe **IP_**. Par exemple : **IP_10.114.24.1**
Default	Indique si l'imprimante est l'imprimante par défaut.

Vous utilisez les boutons qui apparaissent au-dessus des titres de colonne pour ajouter, supprimer et déplacer des lignes et pour enregistrer et importer des entrées de tableau. Chaque bouton a un raccourci clavier équivalent. Passez la souris sur chaque bouton pour en voir une description et son raccourci clavier. Par exemple, pour insérer une ligne à la fin du tableau, cliquez sur le premier bouton du tableau ou appuyez sur Alt+A. Cliquez sur les deux derniers boutons pour importer et enregistrer des entrées de tableau.

Tableau 8-38 montre un exemple de deux lignes de tableau de traduction.

Tableau 8-38. Exemple de paramètre de stratégie de groupe de l'impression basée sur l'emplacement

Plage IP	Nom du client	Adresse Mac	Utilisateur/ Groupe	Nom de l'imprimante	Pilote d'imprimante	IP Port/ThinPrint Port (Port IP/Port ThinPrint)	Default (Valeur par défaut)
*	*	*	*	PRINTER-1-CLR	HP Color LaserJet 4700 PS	IP_10.114.24.1	
10.112.116.140-10.112.116.145	*	*	*	PRINTER-2-CLR	HP Color LaserJet 4700 PS	IP_10.114.24.2	X

L'imprimante en réseau spécifiée sur la première ligne sera mappée vers un poste de travail View de n'importe quel système client car des astérisques apparaissent dans toutes les colonnes de règle de traduction. L'imprimante en réseau spécifiée sur la deuxième ligne sera mappée vers un poste de travail View uniquement si l'adresse IP du système client est comprise dans la plage 10.112.116.140 à 10.112.116.145.

Utilisation de stratégies de groupe Terminal Services

Vous pouvez utiliser des stratégies de groupe Microsoft Windows Terminal Services standard pour contrôler de façon centralisée la configuration de postes de travail View.

Dans les systèmes d'exploitation Windows Vista et supérieurs, les services Terminal Services sont appelés services Bureau à distance.

Remarque Les services Terminal Services doivent être démarrés sur la machine virtuelle que vous utilisez pour créer des pools et sur des postes de travail View. Les services Terminal Services sont requis pour l'installation de View Agent, l'authentification unique et d'autres opérations de gestion des sessions de View.

Pour rechercher des paramètres de stratégie de groupe Terminal Services dans l'Éditeur d'objets de stratégie de groupe, développez le dossier **[Computer Configuration (Configuration ordinateur)]** ou **[User Configuration (Configuration utilisateur)]** , puis développez les dossiers **[Administrative Templates (Modèles administratifs)]** , **[Windows Components (Composants Windows)]** et **[Terminal Services]** .

Paramètres généraux de stratégies de groupe Terminal Services

Les stratégies de groupe Terminal Services générales comportent des paramètres qui contrôlent les comportements d'ouverture et de fermeture de session, les sessions distantes et l'apparence du poste de travail.

Tableau 8-39 décrit les paramètres de stratégie de groupe Terminal Services Configuration d'ordinateur que vous pouvez utiliser pour gérer des postes de travail View.

Tableau 8-39. Paramètres de stratégies Terminal Services générales

Paramètre	Description
`Enforce Removal of Remote Desktop Wallpaper (Forcer la suppression du papier peint du Bureau à distance)`	L'activation de ce paramètre force la suppression du papier peint au cours d'une session distante, ce qui améliore l'expérience utilisateur sur des connexions à faible bande passante.
`Limit maximum color depth (Limiter le nombre maximal de couleurs)`	L'activation de ce paramètre vous permet de spécifier le nombre de couleurs des sessions de poste de travail View.
`Allow users to connect remotely using Terminal Services (Autoriser les utilisateurs à se connecter à distance avec les services Terminal Server)`	L'activation de ce paramètre permet aux utilisateurs de se connecter à distance à l'ordinateur cible.

Tableau 8-39. Paramètres de stratégies Terminal Services générales (suite)

Paramètre	Description
Remove Windows Security item from Start Menu (Supprimer l'option Sécurité Windows du menu Démarrer)	La désactivation de ce paramètre fait apparaître l'élément Sécurité Windows dans le menu Settings (Paramètres), ce qui garantit que les utilisateurs ont un mécanisme de fermeture de session.
Remove Disconnect option from Shut Down dialog (Supprimer l'élément Déconnecter de la boîte de dialogue Arrêter)	L'activation de ce paramètre supprime l'option Disconnect (Déconnecter) de la boîte de dialogue Shut Down (Arrêter) de Windows, ce qui réduit la possibilité pour les utilisateurs de se déconnecter au lieu de fermer leur session.

Paramètres de stratégie de groupe Terminal Services pour des sessions

Les paramètres de stratégie de groupe Terminal Services pour des sessions incluent des paramètres qui contrôlent les sessions client déconnectées et inactives.

Tableau 8-40 décrit les paramètres de stratégie de groupe Terminal Services Configuration d'ordinateur et Configuration d'utilisateur que vous pouvez utiliser pour gérer des propriétés liées aux sessions pour des postes de travail View et des utilisateurs.

Tableau 8-40. Paramètres de stratégie Terminal Services pour des sessions

Paramètre	Description
Set time limit for disconnected sessions (Définir une limite pour les sessions déconnectées)	Activer ce paramètre vous permet de définir une limite de temps pour les sessions déconnectées. Les sessions déconnectées sont fermées après la limite de temps spécifiée.
Sets a time limit for active but idle Terminal Services sessions (Définit une limite de temps pour les sessions Terminal Services inactives)	Activer ce paramètre vous permet de définir une limite de temps pour les sessions inactives. Les sessions inactives sont fermées après la limite de temps spécifiée.

Vous pouvez combiner ces paramètres avec des règles d'alimentation de poste de travail View pour créer une solution dynamique afin d'interrompre ou de mettre hors tension des postes de travail View déconnectés. Lorsque des postes de travail View sont interrompus ou mis hors tension, les ressources deviennent disponibles pour les autres postes de travail.

Exemple de stratégie de groupe Active Directory

L'une des façons d'implémenter des stratégies de groupe Active Directory dans View est de créer une UO pour vos postes de travail View et de lier un ou plusieurs GPO à cette UO. Vous pouvez utiliser ces GPO pour appliquer des paramètres de stratégie de groupe à vos postes de travail View et activer le traitement en boucle.

Vous pouvez configurer des stratégies sur votre serveur Active Directory ou sur n'importe quel ordinateur de votre domaine. Cet exemple montre comment configurer des stratégies directement sur votre serveur Active Directory.

Remarque Comme chaque environnement View est différent, vous devrez peut-être effectuer différentes étapes pour répondre aux besoins spécifiques de votre entreprise.

Procédure

1 Créer une UO pour des postes de travail View page 256

Pour appliquer des stratégies de groupe à des postes de travail View sans affecter d'autres ordinateurs Windows dans le même domaine Active Directory, créez une UO spécifiquement pour vos postes de travail View.

2 Créer des GPO pour les stratégies de groupe View page 256

Créez des GPO pour contenir des stratégies de groupe pour des composants View et l'impression basée sur l'emplacement et les lier à l'UO de vos postes de travail View.

3 Ajouter des modèles d'administration View à un GPO page 257

Pour appliquer des paramètres de stratégie de groupe de composant View à vos postes de travail View, ajoutez leurs fichiers de modèle d'administration à des GPO.

4 Activer le traitement en boucle pour des postes de travail View page 258

Pour appliquer des paramètres de Configuration d'utilisateur qui s'appliquent généralement à un ordinateur à tous les utilisateurs qui ouvrent une session sur cet ordinateur, activez le traitement en boucle.

Créer une UO pour des postes de travail View

Pour appliquer des stratégies de groupe à des postes de travail View sans affecter d'autres ordinateurs Windows dans le même domaine Active Directory, créez une UO spécifiquement pour vos postes de travail View.

Procédure

1 Sur votre serveur Active Directory, sélectionnez **[Start (Démarrer)] > [All Programs (Tous les programmes)] > [Administrative Tools (Outils d'administration)] > [Active Directory Users and Computers (Utilisateurs et ordinateurs Active Directory)]** .

2 Cliquez avec le bouton droit sur le domaine qui contient vos postes de travail View et sélectionnez **[New (Nouveau)] > [Organizational Unit (Unité d'organisation)]** .

3 Saisissez un nom pour l'UO et cliquez sur **[OK]** .

La nouvelle UO apparaît dans le volet de gauche.

4 Pour ajouter des postes de travail View à la nouvelle UO :

a Cliquez sur **[Computers (Ordinateurs)]** dans le volet de gauche.

Tous les objets ordinateur dans le domaine apparaissent dans le volet de droite.

b Cliquez avec le bouton droit sur le nom de l'objet ordinateur qui représente le poste de travail View dans le volet de droite et sélectionnez **[Move (Déplacer)]** .

c Sélectionnez l'UO et cliquez sur **[OK]** .

Le poste de travail View apparaît dans le volet de droite lorsque vous sélectionnez l'UO.

Suivant

Créez des GPO pour les stratégies de groupe View.

Créer des GPO pour les stratégies de groupe View

Créez des GPO pour contenir des stratégies de groupe pour des composants View et l'impression basée sur l'emplacement et les lier à l'UO de vos postes de travail View.

Prérequis

- Créez une UO pour vos postes de travail View.
- Vérifiez que les composants logiciels enfichables Microsoft MMC et que l'Éditeur d'objets de stratégie de groupe sont disponibles sur votre serveur Active Directory.

Procédure

1 Dans le serveur Active Directory, accédez à l'UO et ouvrez l'éditeur GPO.

Version AD	Chemin de navigation
Windows 2003	a Sélectionnez **[Start (Démarrer)] > [All Programs (Tous les programmes)] > [Administrative Tools (Outils d'administration)] > [Active Directory Users and Computers (Utilisateurs et ordinateurs Active Directory)]** . b Cliquez avec le bouton droit sur l'UO qui contient vos postes de travail View et sélectionnez **[Properties (Propriétés)]** . c Sous l'onglet **[Group Policy (Stratégie de groupe)]** , cliquez sur **[Open (Ouvrir)]** pour ouvrir le plug-in Group Policy Management (Gestion de stratégie de groupe). d Cliquez avec le bouton droit sur l'UO et sélectionnez **[Create and Link a GPO Here (Créer et lier un GPO ici)]** .
Windows 2008	a Sélectionnez **[Start (Démarrer)] > [Administrative Tools (Outils d'administration)] > [Group Policy Management (Gestion de stratégie de groupe)]** . b Développez votre domaine, cliquez avec le bouton droit de la souris sur l'UO qui contient les postes de travail View, puis sélectionnez **[Create and Link a GPO Here (Créer et lier un GPO ici)]** .

2 Saisissez un nom pour le GPO et cliquez sur **[OK]** .

Le nouveau GPO apparaît sous l'UO dans le volet de gauche.

3 (Facultatif) Pour appliquer le GPO uniquement à des postes de travail View spécifiques dans l'UO :

a Sélectionnez le GPO dans le volet de gauche.

b Sélectionnez **[Security Filtering (Filtrage de sécurité)] > [Ajouter]** .

c Saisissez les noms d'ordinateur des postes de travail View et cliquez sur **[OK]** .

Les postes de travail View apparaissent dans le volet Security Filtering (Filtrage de sécurité). Les paramètres dans le GPO ne s'appliquent qu'à ces postes de travail View.

Suivant

Ajoutez les modèles d'administration View au GPO pour des stratégies de groupe.

Ajouter des modèles d'administration View à un GPO

Pour appliquer des paramètres de stratégie de groupe de composant View à vos postes de travail View, ajoutez leurs fichiers de modèle d'administration à des GPO.

Prérequis

- Créez des GPO pour les paramètres de stratégie de groupe du composant View et liez-les à l'UO qui contient vos postes de travail View.
- Vérifiez que les composants logiciels enfichables Microsoft MMC et que l'Éditeur d'objets de stratégie de groupe sont disponibles sur votre serveur Active Directory.

Procédure

1 Copiez les fichiers de modèle d'administration de composant View du répertoire *install_directory*\VMware\VMware View\Server\extras\GroupPolicyFiles de votre hôte de Serveur de connexion View vers votre serveur Active Directory.

2 Sur le serveur Active Directory, modifiez le GPO.

Version AD	Chemin de navigation
Windows 2003	a Sélectionnez **[Start (Démarrer)] > [All Programs (Tous les programmes)] > [Administrative Tools (Outils d'administration)] > [Active Directory Users and Computers (Utilisateurs et ordinateurs Active Directory)]** . b Cliquez avec le bouton droit sur l'UO qui contient vos postes de travail View et sélectionnez **[Properties (Propriétés)]** . c Sous l'onglet **[Group Policy (Stratégie de groupe)]** , cliquez sur **[Open (Ouvrir)]** pour ouvrir le plug-in Group Policy Management (Gestion de stratégie de groupe). d Dans le volet de droite, cliquez avec le bouton droit sur le GPO que vous avez créé pour les paramètres de stratégie de groupe et sélectionnez **[Edit (Modifier)]** .
Windows 2008	a Sélectionnez **[Start (Démarrer)] > [Administrative Tools (Outils d'administration)] > [Group Policy Management (Gestion de stratégie de groupe)]** . b Développez votre domaine, cliquez avec le bouton droit sur le GPO que vous avez créé pour les paramètres de stratégie de groupe et sélectionnez **[Edit (Modifier)]** .

La fenêtre Group Policy Object Editor (Éditeur d'objets de stratégie de groupe) apparaît.

3 Dans l'Éditeur d'objets de stratégie de groupe, cliquez avec le bouton droit sur **[Administrative Templates (Modèles administratifs)]** sous **[Computer Configuration (Configuration ordinateur)]** et sélectionnez **[Add/Remove Templates (Ajout/Suppression de modèles)]** .

4 Cliquez sur **[Add (Ajouter)]** , recherchez le fichier de modèle d'administration et cliquez sur **[Open (Ouvrir)]** .

5 Cliquez sur **[Close (Fermer)]** pour appliquer les paramètres de stratégie dans le fichier de modèle d'administration au GPO.

Le nom du modèle apparaît dans le volet gauche sous **[Administrative Templates (Modèles administratifs)]** .

6 Configurez les paramètres de stratégie de groupe.

Suivant

Activez le traitement en boucle pour vos postes de travail View.

Activer le traitement en boucle pour des postes de travail View

Pour appliquer des paramètres de Configuration d'utilisateur qui s'appliquent généralement à un ordinateur à tous les utilisateurs qui ouvrent une session sur cet ordinateur, activez le traitement en boucle.

Prérequis

- Créez des GPO pour les paramètres de stratégie de groupe du composant View et liez-les à l'UO qui contient vos postes de travail View.
- Vérifiez que les composants logiciels enfichables Microsoft MMC et que l'Éditeur d'objets de stratégie de groupe sont disponibles sur votre serveur Active Directory.

Procédure

1 Sur le serveur Active Directory, modifiez l'objet de stratégie de groupe.

Version AD	Chemin de navigation
Windows 2003	a Sélectionnez **[Start (Démarrer)] > [All Programs (Tous les programmes)] > [Administrative Tools (Outils d'administration)] > [Active Directory Users and Computers (Utilisateurs et ordinateurs Active Directory)]** . b Cliquez avec le bouton droit sur l'UO qui contient vos postes de travail View et sélectionnez **[Properties (Propriétés)]** . c Sous l'onglet **[Group Policy (Stratégie de groupe)]** , cliquez sur **[Open (Ouvrir)]** pour ouvrir le plug-in Group Policy Management (Gestion de stratégie de groupe). d Dans le volet de droite, cliquez avec le bouton droit de la souris sur le GPO que vous avez créé pour les paramètres de stratégie de groupe et sélectionnez **[Edit (Modifier)]** .
Windows 2008	a Sélectionnez **[Start (Démarrer)] > [Administrative Tools (Outils d'administration)] > [Group Policy Management (Gestion de stratégie de groupe)]** . b Développez votre domaine, cliquez dans le volet, cliquez avec le bouton droit de la souris sur l'objet de stratégie de groupe (GPO) que vous avez créé pour les paramètres de stratégie de groupe et sélectionnez **[Edit (Modifier)]** .

La fenêtre Group Policy Object Editor (Éditeur d'objets de stratégie de groupe) apparaît.

2 Développez le dossier **[Computer Configuration (Configuration ordinateur)]** , puis les dossiers **[Administrative Templates (Modèles administratifs)]** , **[System (Système)]** et **[Group Policy (Stratégie de groupe)]** .

3 Dans le volet de droite, cliquez avec le bouton droit sur **[User Group Policy loopback processing mode (Mode de traitement en boucle de la stratégie de groupe d'utilisateurs)]** et sélectionnez **[Properties (Propriétés)]** .

4 Sous l'onglet **[Setting (Paramètre)]** , sélectionnez **[Enabled (Activé)]** puis sélectionnez un mode de traitement en boucle dans le menu déroulant **[Mode]** .

Option	Action
Merge (Fusionner)	Les paramètres de règle utilisateur appliqués sont la combinaison de ceux inclus dans les GPO ordinateur et utilisateur. En cas de conflit, les GPO ordinateur sont prioritaires.
Replace (Remplacer)	La règle utilisateur est définie entièrement depuis les GPO associés à l'ordinateur. Tous les GPO associés à l'utilisateur sont ignorés.

5 Cliquez sur **[OK]** pour enregistrer vos modifications.

Configuration de profils d'utilisateur avec View Persona Management (Gestion de Persona View)

9

Avec View Persona Management (Gestion de Persona View), vous pouvez configurer des profils d'utilisateur qui sont synchronisés dynamiquement avec un référentiel de profils distant. Cette fonction permet à l'utilisateur d'avoir une expérience de poste de travail personnalisée lorsqu'il ouvre une session sur un poste de travail. Gestion de persona View étend la fonctionnalité et améliore les performances des profils d'itinérants Windows, mais ne nécessite pas que les profils d'itinérants Windows fonctionnent.

Vous configurez des paramètres de stratégie de groupe pour activer Gestion de persona View et contrôler plusieurs aspects de votre déploiement de Gestion de persona View.

Pour activer et utiliser View Persona Management (Gestion de Persona View), vous devez posséder une licence View Premier. Consultez le Contrat de licence d'utilisateur final (CLUF) de VMware à l'adresse http://www.vmware.com/download/eula.

Ce chapitre aborde les rubriques suivantes :

Fournir des personas d'utilisateur dans View

Avec la fonction de View Persona Management, le profil distant d'un utilisateur est téléchargé dynamiquement lorsque l'utilisateur ouvre une session sur un poste de travail View. Vous pouvez configurer View pour stocker des profils d'utilisateur dans un référentiel sécurisé et centralisé. View télécharge des informations sur le persona quand l'utilisateur en a besoin.

View Persona Management est une alternative aux profils itinérants de Windows. View Persona Management développe la fonctionnalité et améliore les performances par rapport aux profils itinérants de Windows.

Vous pouvez configurer et gérer entièrement des personas dans View. Vous n'avez pas à configurer les profils itinérants de Windows. Si vous avez une configuration de profils itinérants de Windows, vous pouvez utiliser votre configuration de référentiel existante avec View.

Un profil d'utilisateur est indépendant du poste de travail virtuel. Lorsqu'un utilisateur ouvre une session sur un poste de travail, le même profil apparaît.

Par exemple, un utilisateur peut ouvrir une session sur un pool de clone lié d'affectation flottante et modifier l'arrière-plan du poste de travail et les paramètres de Microsoft Word. Lorsque l'utilisateur démarre la prochaine session, la machine virtuelle est différente, mais l'utilisateur voit les mêmes paramètres.

Un profil d'utilisateur comporte plusieurs informations générées par l'utilisateur :

- des données spécifiques à l'utilisateur et des paramètres de poste de travail ;
- des données et des paramètres d'application ;
- des entrées de registre de Windows configurées par des applications utilisateur.

De plus, si vous approvisionnez des postes de travail avec des applications ThinApp, les données de sandbox ThinApp peuvent être stockées dans le profil d'utilisateur et déplacées avec l'utilisateur.

View Persona Management minimise le temps nécessaire pour ouvrir et fermer une session sur des postes de travail. La durée d'ouverture et de fermeture de session peut être problématique avec les profils itinérants de Windows.

- Lors de l'ouverture de session, View télécharge uniquement les fichiers dont Windows a besoin, tels que les fichiers de registre utilisateur. Les autres fichiers sont copiés vers le poste de travail local quand l'utilisateur ou une application les ouvre depuis le dossier de profil local.
- View copie les modifications récentes dans le profil local sur le référentiel distant, en général avec des intervalles de quelques minutes. La valeur par défaut est toutes les 10 minutes. Vous pouvez spécifier la fréquence de chargement du profil local.
- Lors de la fermeture de session, seuls les fichiers qui ont été mis à jour depuis la dernière réplication sont copiés dans le référentiel distant.

Utilisation de View Persona Management avec des systèmes autonomes

Vous pouvez installer une version autonome de View Persona Management sur des ordinateurs physiques et des machines virtuelles qui ne sont pas gérés par View. Avec ce logiciel, vous pouvez gérer des profils d'utilisateur sur des postes de travail View et des systèmes autonomes.

Le logiciel View Persona Management autonome fonctionne sur les systèmes d'exploitation Windows XP SP3, Windows Vista, Windows 7 et Windows 8.

Vous pouvez utiliser le logiciel View Persona Management autonome pour réaliser les objectifs suivants :

- Partager des profils d'utilisateur sur des systèmes autonomes et des postes de travail View

  Vos utilisateurs peuvent continuer à utiliser des systèmes autonomes ainsi que des postes de travail View avec View Persona Management. Si vous utilisez les mêmes paramètres de stratégie de groupe View Persona Management pour contrôler des postes de travail View et des systèmes physiques, les utilisateurs peuvent recevoir leurs profils actualisés à chaque fois qu'ils ouvrent une session, qu'ils utilisent leurs ordinateurs hérités ou des postes de travail View.

  Remarque View Persona Management ne prend pas en charge les sessions actives simultanées. Un utilisateur doit fermer sa session avant d'en ouvrir une autre.

- Migrer des profils d'utilisateur entre des systèmes physiques et des postes de travail View

  Si vous prévoyez de requalifier des ordinateurs physiques hérités à utiliser dans un déploiement de View, vous pouvez installer View Persona Management autonome sur les systèmes hérités avant de restaurer les postes de travail View pour vos utilisateurs. Lorsque les utilisateurs ouvrent une session sur leurs systèmes hérités, leurs profils sont stockés sur le référentiel de profils distant View. Lorsque les utilisateurs ouvrent une session sur leurs postes de travail View pour la première fois, leurs profils existants sont téléchargés sur leurs postes de travail View.

- Effectuer une migration par étape entre des systèmes physiques et des postes de travail View

Si vous migrez votre déploiement par étape, les utilisateurs qui n'ont pas encore accès à des postes de travail View peuvent utiliser View Persona Management autonome. À mesure que chaque jeu de postes de travail View est déployé, les utilisateurs peuvent accéder à leurs profils sur leurs postes de travail View et les systèmes hérités peuvent être supprimés progressivement. Ce scénario est un hybride des scénarios précédents.

- Prendre en charge des profils actualisés lorsque les utilisateurs ferment leur session

  Les utilisateurs d'ordinateurs portables autonomes peuvent se déconnecter du réseau. Lorsqu'un utilisateur se reconnecte, View Persona Management charge les dernières modifications dans le profil local de l'utilisateur vers le référentiel de profils distant.

Remarque Pour qu'un utilisateur puisse se déconnecter, le profil d'utilisateur doit être complètement téléchargé sur le système local.

Migration de profils d'utilisateur avec View Persona Management

Avec View Persona Management, vous pouvez migrer des profils d'utilisateur existants dans plusieurs paramètres vers des postes de travail View. Lorsque les utilisateurs ouvrent une session sur leurs postes de travail View après une migration de profil, ils voient les paramètres et données personnels qu'ils ont utilisés sur leurs systèmes hérités.

En migrant des profils d'utilisateur, vous pouvez atteindre les objectifs de migration de poste de travail suivants :

- Vous pouvez mettre à niveau les systèmes de vos utilisateurs de Windows XP à Windows 7 ou Windows 8 et migrer vos utilisateurs d'ordinateurs physiques vers View pour la première fois.
- Dans un déploiement de View existant, vous pouvez effectuer une mise à niveau de postes de travail View Windows XP vers des postes de travail View Windows 7 ou Windows 8.
- Vous pouvez effectuer une migration entre des ordinateurs physiques et des postes de travail View sans mettre à niveau les systèmes d'exploitation.

Pour réaliser ces scénarios, View Persona Management fournit un utilitaire de migration de profil et un programme d'installation View Persona Management autonome pour les machines physiques ou virtuelles sur lesquelles View Agent 5.*x* n'est pas installé.

Le Tableau 9-1 montre différents scénarios de migration et présente les tâches que vous devez effectuer dans chaque scénario.

Tableau 9-1. Scénarios de migration de profil d'utilisateur

S'il s'agit de votre déploiement d'origine...	Et s'il s'agit de votre déploiement de destination...	Effectuez les tâches suivantes :
Ordinateurs physiques Windows XP	Postes de travail View Windows 7 ou Windows 8	1 Configurez les postes de travail View Windows 7 ou Windows 8 avec View Persona Management pour vos utilisateurs. Reportez-vous à la section « Configuration d'un déploiement de Gestion de Persona View », page 266. **Remarque** Ne restaurez pas les postes de travail View Windows 7 ou Windows 8 pour vos utilisateurs avant d'avoir effectué l'étape 2. 2 Exécutez l'utilitaire de migration de profil View V1 à V2. ■ Pour les profils source, spécifiez les profils locaux sur les ordinateurs physiques Windows XP. ■ Pour les profils de destination, spécifiez le référentiel de profils distant que vous avez configuré pour le déploiement de View. Pour plus d'informations, consultez le document *Migration des profils d'utilisateur VMware Horizon View*. 3 Autorisez vos utilisateurs à ouvrir une session sur leurs postes de travail View Windows 7 ou Windows 8.
Ordinateurs physiques ou machines virtuelles Windows XP qui utilisent une solution de profil d'utilisateur itinérant. Par exemple, votre déploiement peut utiliser l'une des solutions suivantes : ■ View Persona Management ■ RTO Virtual Profiles ■ profils itinérants de Windows Dans ce scénario, les profils d'utilisateur d'origine doivent être conservés dans un référentiel de profils distant.	Postes de travail View Windows 7 ou Windows 8	1 Configurez les postes de travail View Windows 7 ou Windows 8 avec View Persona Management pour vos utilisateurs. Reportez-vous à la section « Configuration d'un déploiement de Gestion de Persona View », page 266. **Remarque** Ne restaurez pas les postes de travail View Windows 7 ou Windows 8 pour vos utilisateurs avant d'avoir effectué l'étape 2. 2 Exécutez l'utilitaire de migration de profil View V1 à V2. ■ Pour les profils source, spécifiez le référentiel de profils distant pour les systèmes Windows XP. ■ Pour les profils de destination, spécifiez le référentiel de profils distant que vous avez configuré pour le déploiement de View. Pour plus d'informations, consultez le document *Migration des profils d'utilisateur VMware Horizon View*. 3 Autorisez vos utilisateurs à ouvrir une session sur leurs postes de travail View Windows 7.

Tableau 9-1. Scénarios de migration de profil d'utilisateur (suite)

S'il s'agit de votre déploiement d'origine...	Et s'il s'agit de votre déploiement de destination...	Effectuez les tâches suivantes :
Ordinateurs physiques ou machines virtuelles Windows XP. View Agent 5.*x* ne peut pas être installé sur les systèmes hérités.	Postes de travail View Windows XP	1 Configurez des postes de travail View Windows XP avec View Persona Management pour vos utilisateurs. Reportez-vous à la section « Configuration d'un déploiement de Gestion de Persona View », page 266. 2 Installez le logiciel View Persona Management autonome sur les systèmes Windows XP. Reportez-vous à la section « Installer View Persona Management autonome », page 270. 3 Configurez les systèmes Windows XP hérités pour utiliser le même référentiel de profils distant que les postes de travail View. Reportez-vous à la section « Configurer un référentiel de profils d'utilisateur », page 267. L'approche la plus facile consiste à utiliser les mêmes paramètres de stratégie de groupe View Persona Management dans Active Directory pour contrôler les systèmes hérités et les postes de travail View. Reportez-vous à la section « Ajouter le fichier de modèle d'administration de View Persona Management (Gestion de Persona View) », page 271. 4 Restaurez vos postes de travail View Windows XP pour vos utilisateurs.
Ordinateurs physiques ou machines virtuelles Windows 7 ou Windows 8. View Agent 5.*x* ne peut pas être installé sur les systèmes hérités.	Postes de travail View Windows 7 ou Windows 8	1 Configurez les postes de travail View Windows 7 ou Windows 8 avec View Persona Management pour vos utilisateurs. Reportez-vous à la section « Configuration d'un déploiement de Gestion de Persona View », page 266. 2 Installez le logiciel View Persona Management autonome sur les systèmes Windows 7 ou Windows 8. Reportez-vous à la section « Installer View Persona Management autonome », page 270. 3 Configurez les systèmes Windows 7 ou Windows 8 hérités pour utiliser le même référentiel de profils distant que les postes de travail View. Reportez-vous à la section « Configurer un référentiel de profils d'utilisateur », page 267. L'approche la plus facile consiste à utiliser les mêmes paramètres de stratégie de groupe View Persona Management dans Active Directory pour contrôler les systèmes hérités et les postes de travail View. Reportez-vous à la section « Ajouter le fichier de modèle d'administration de View Persona Management (Gestion de Persona View) », page 271. 4 Restaurez vos postes de travail View Windows 7 ou Windows 8 pour vos utilisateurs.

Persona Management et profils itinérants de Windows

Lorsque Persona Management est activé, vous ne pouvez pas modifier les personas des utilisateurs de View en utilisant les fonctions des profils itinérants de Windows.

Par exemple, si vous ouvrez une session sur le système d'exploitation client d'un poste de travail, allez à l'onglet **[Advanced (Avancé)]** dans la boîte de dialogue System Properties (Propriétés système) et modifiez les paramètres User Profiles (Profils d'utilisateur) de **[Roaming profile (Profil itinérant)]** à **[Local profile (Profil local)]** . View Persona Management continue de synchroniser le persona de l'utilisateur entre le poste de travail local et le référentiel de persona distant.

Toutefois, vous pouvez spécifier des fichiers et des dossiers dans les personas des utilisateurs qui sont gérés par la fonctionnalité de profils itinérants de Windows plutôt que par View Persona Management. Vous utilisez la stratégie **[Windows Roaming Profiles Synchronization (Synchronisation de profils itinérants de Windows)]** pour spécifier ces fichiers et dossiers.

Configuration d'un déploiement de Gestion de Persona View

Pour configurer Gestion de persona View, vous configurez un référentiel distant qui stocke des profils d'utilisateur, installez View Agent avec l'option d'installation **[Gestion de persona View]** sur des postes de travail de machine virtuelle, ajoutez et configurez des paramètres de stratégie de groupe Gestion de persona View et déployez des pools de postes de travail.

Vous pouvez également configurer View Persona Management (Gestion de persona View) pour un déploiement non-View. Vous installez la version autonome de Gestion de persona View sur les ordinateurs portables, les ordinateurs de bureau ou les machines virtuelles des utilisateurs. Vous devez également installer un référentiel distant et définir les paramètres de stratégie de groupe Gestion de persona View.

Présentation de la configuration d'un déploiement de Gestion de persona View

Pour configurer un déploiement de poste de travail View ou d'ordinateurs automes avec Gestion de persona View, vous devez exécuter plusieurs tâches générales.

Cet ordre est recommandé, mais vous pouvez réaliser ces tâches dans un ordre différent. Par exemple, vous pouvez configurer ou reconfigurer des paramètres de stratégie de groupe dans Active Directory une fois que vous avez déployé des pools de postes de travail.

1 Configurez un référentiel distant pour stocker des profils d'utilisateur.

  Vous pouvez configurer un partage de réseau ou utiliser un chemin de profil d'utilisateur Active Directory existant que vous avez configuré pour des profils itinérants de Windows.

2 Installez View Agent avec l'option d'installation **[Gestion de persona View]** sur les machines virtuelles que vous utilisez pour créer des pools de postes de travail.

  Pour configurer Gestion de persona View pour des ordinateurs portables, des ordinateurs de bureau ou des machines virtuelles non-View, installez le logiciel Gestion de persona View autonome sur chaque ordinateur de l'environnement cible.

3 Ajoutez le fichier de modèle d'administration de Gestion de persona View à votre serveur Active Directory ou à la configuration Stratégie Ordinateur local sur la machine virtuelle parente.

  Pour configurer Gestion de persona View pour l'ensemble du déploiement View ou non-View, ajoutez le modèle de fichier ADM à Active Directory.

  Pour configurer Gestion de persona View pour un pool de postes de travail, vous pouvez suivre ces approches :

  - Ajoutez le fichier de modèle d'administration à la machine virtuelle que vous utilisez pour créer le pool.

- Ajoutez le fichier de modèle d'administration à Active Directory et appliquez les paramètres de stratégie de groupe à l'UO qui contient les postes de travail dans le pool.

4 Activez Gestion de persona View en activant le paramètre de stratégie de groupe **[Manage user persona (Gérer un persona d'utilisateur)]** .

5 Si vous avez configuré un partage de réseau pour le référentiel de profils distant, activez le paramètre de stratégie de groupe **[Persona repository location (Emplacement du référentiel de persona)]** et spécifiez le chemin du partage de réseau.

6 (Facultatif) Configurez d'autres paramètres de stratégie de groupe dans Active Directory ou dans la configuration Stratégie Ordinateur local.

7 Créez des pools de postes de travail à partir des machines virtuelles sur lesquelles vous avez installé View Agent avec l'option d'installation **[Gestion de persona View]** .

Configurer un référentiel de profils d'utilisateur

Vous pouvez configurer un référentiel distant pour stocker des données et des paramètres d'utilisateur, des données spécifiques de l'application et d'autres informations générées par l'utilisateur dans des profils d'utilisateur. Si des profils itinérants de Windows sont configurés dans votre déploiement, vous pouvez utiliser un chemin de profil d'utilisateur Active Directory existant à la place.

Remarque Vous pouvez configurer Gestion de persona View sans avoir à configurer des profils itinérants de Windows.

Prérequis

Familiarisez-vous avec les recommandations sur la création d'un référentiel de profils d'utilisateur. Reportez-vous à la section « Création d'un partage de réseau pour View Persona Management », page 268.

Procédure

1 Déterminez si vous voulez utiliser un chemin de profil d'utilisateur Active Directory existant ou configurer un référentiel de profils d'utilisateur sur un partage de réseau.

Option	Action
Use an existing Active Directory user profile path (Utiliser un chemin de profil d'utilisateur Active Directory)	Si vous possédez une configuration de profils itinérants de Windows existante, vous pouvez utiliser le chemin de profil d'utilisateur dans Active Directory qui prend en charge les profils itinérants. Vous pouvez ignorer les étapes restantes de cette procédure.
Configure a network share to store the user profile repository (Configurer un partage de réseau pour stocker le référentiel de profils d'utilisateur)	Si vous ne possédez pas de configuration de profils itinérants de Windows existante, vous devez configurer un partage de réseau pour le référentiel de profils d'utilisateur. Suivez les étapes restantes de cette procédure.

2 Créez un dossier partagé sur un ordinateur auquel vos utilisateurs peuvent accéder depuis les Systèmes d'exploitation clients sur leurs postes de travail.

Si `%username%` ne fait pas partie du chemin de dossier que vous configurez, Gestion de persona View ajoute `%username%.%userdomain%` au chemin.

Par exemple : `\\server.domain.com\VPRepository\%username%.%userdomain%`

3 Définissez des autorisations d'accès pour les dossiers partagés qui contiennent des profils d'utilisateur.

Définissez les autorisations que vous utiliseriez pour configurer la sécurité pour des profils itinérants de Windows. Pour plus d'informations, consultez la rubrique de Microsoft TechNet, *Security Recommendations for Roaming User Profiles Shared Folders (Recommandations de sécurité pour les dossiers partagés de profils d'utilisateur itinérants)*. http://technet.microsoft.com/en-us/library/cc757013(WS.10).aspx

La rubrique *Recommandations de sécurité pour les dossiers partagés des profils d'utilisateur itinérants* répertorie les autorisations minimales suivantes pour les groupes d'utilisateurs de sécurité devant placer des données dans le partage : **Lister les dossiers/Lire les données** et **Créer des dossiers/Ajouter les données - Ce dossier seulement**.

Pour pouvoir ajouter le dossier `%username%.%userdomain%` au partage de réseau, vous devez définir également l'autorisation **Lire les attributs** .

Création d'un partage de réseau pour View Persona Management

Vous devez suivre certaines recommandations lorsque vous créez un dossier partagé à utiliser en tant que référentiel de profils.

- Si vous utilisez des postes de travail Windows 8 et que votre partage réseau utilise un système de fichiers OneFS sur un périphérique NAS EMC Isilon, la version du système de fichiers OneFS doit être 6.5.5.11 ou supérieure.
- Vous pouvez créer le dossier partagé sur un serveur, un périphérique NAS (Network Attached Storage) ou un serveur réseau.
- Le dossier partagé n'a pas à être dans le même domaine que Serveur de connexion View.
- Le dossier partagé doit se trouver dans la même forêt Active Directory que celle des utilisateurs qui stockent des profils dans le dossier partagé.
- Vous devez utiliser un lecteur partagé suffisamment volumineux pour stocker des informations de profil d'utilisateur pour vos utilisateurs. Pour prendre en charge un déploiement volumineux de View, vous pouvez configurer des référentiels séparés pour différents pools de postes de travail.

  Si des utilisateurs sont autorisés à accéder à plusieurs pools, les pools qui partagent des utilisateurs doivent être configurés avec le même référentiel de profils. Si vous autorisez un utilisateur à accéder à deux pools avec deux référentiels de profils différents, l'utilisateur ne peut pas accéder à la même version du profil depuis des postes de travail dans chaque pool.
- Vous devez créer le chemin de profil complet sous lequel les dossiers de profils d'utilisateur seront créés. Si une partie du chemin n'existe pas, Windows crée les dossiers manquants lorsque le premier utilisateur ouvre une session, puis affecte des restrictions de sécurité de l'utilisateur à ces dossiers. Windows affecte les mêmes restrictions de sécurité à tous les dossiers qu'il crée dans ce chemin.

  Par exemple, pour `user1`, vous pouvez configurer le chemin View Persona Management `\\server\VPRepository\profiles\user1`. Si vous créez le partage de réseau `\\server\VPRepository`, et si le dossier `profiles` n'existe pas, Windows crée le chemin `\profiles\user1` lorsque `user1` ouvre une session. Windows limite l'accès aux dossiers `\profiles\user1` au compte `user1`. Si un autre utilisateur ouvre une session avec un chemin de profil dans `\\server\VPRepository\profiles`, le deuxième utilisateur ne peut pas accéder au référentiel et la réplication du profil de l'utilisateur échoue.

Installer View Agent avec l'option View Persona Management

Pour utiliser View Persona Management avec des postes de travail View, vous devez installer View Agent avec l'option d'installation **[Gestion de persona View]** sur les machines virtuelles que vous utilisez pour créer des pools de postes de travail.

Pour un pool automatisé, vous installez View Agent avec l'option d'installation **[View Persona Management]** sur la machine virtuelle que vous utilisez en tant que parent ou modèle. Lorsque vous créez un pool de postes de travail à partir de la machine virtuelle, le logiciel View Persona Management est déployé sur vos postes de travail View.

Pour un pool manuel, vous devez installer View Agent avec l'option d'installation **[View Persona Management]** sur chaque machine virtuelle utilisée en tant que source de postes de travail dans le pool. Utilisez Active Directory pour configurer des stratégies de groupe View Persona Management pour un pool manuel. L'autre solution consiste à ajouter le fichier de modèle d'administration et à configurer des stratégies de groupe sur chaque source de postes de travail individuelle.

Remarque Un utilisateur ne peut pas accéder au même profil si l'utilisateur bascule entre des postes de travail qui ont des profils d'utilisateur v1 et v2. Windows XP utilise les profils v1. Windows 8 et Windows 7 utilisent des profils v2.

Par exemple, si un utilisateur ouvre une session sur un poste de travail Windows XP puis sur un poste de travail Windows 7, la machine virtuelle Windows 7 ne peut pas lire le profil v1 qui a été créé lors de la session de poste de travail Windows XP.

Vous pouvez utiliser l'utilitaire de ligne de commande de migration de profil View pour migrer des profils Windows XP vers des profils Windows 7 ou Windows 8. Consultez le document *Migration des profils d'utilisateur VMware Horizon View*.

Prérequis

- Vérifiez que vous effectuez l'installation sur une machine virtuelle Windows 8, Windows 7, Windows Vista ou Windows XP. View Persona Management ne fonctionne pas sur des serveurs Microsoft Terminal Server.

  L'installation de View Agent avec l'option d'installation **[View Persona Management]** ne fonctionne pas sur les ordinateurs physiques. Vous pouvez installer le logiciel View Persona Management autonome sur des ordinateurs physiques. Reportez-vous à la section « Installer View Persona Management autonome », page 270.

- Vérifiez que vous pouvez ouvrir une session en tant qu'administrateur sur la machine virtuelle.
- Vérifiez que le service natif RTO Virtual Profiles 2.0 n'est pas installé sur la machine virtuelle. Si un service natif RTO Virtual Profile 2.0 est présent, désinstallez-le avant d'installer View Agent avec l'option d'installation **[View Persona Management]** .
- Sur des machines virtuelles Windows XP, téléchargez et installez le service UPHClean (User Profile Hive Cleanup) de Microsoft sur le système d'exploitation client. Reportez-vous à la section « Installation de UPHClean sur des postes de travail Windows XP qui utilisent Gestion de persona View », page 270.
- Familiarisez-vous avec l'installation de View Agent. Reportez-vous à la section « Installer View Agent sur une machine virtuelle », page 71 ou « Installer View Agent sur une source de postes de travail non gérée », page 62.

Procédure

- Lorsque vous installez View Agent sur une machine virtuelle, sélectionnez l'option d'installation **[View Persona Management]** .

Suivant

Ajoutez le fichier de modèle d'administration de View Persona Management à votre serveur Active Directory ou à la configuration Stratégie Ordinateur local sur la machine virtuelle elle-même. Reportez-vous à la section « Ajouter le fichier de modèle d'administration de View Persona Management (Gestion de Persona View) », page 271.

Installation de UPHClean sur des postes de travail Windows XP qui utilisent Gestion de persona View

Le service UPHClean (User Profile Hive Cleanup) de Microsoft garantit que les sessions utilisateur sont complètement terminées lorsqu'un utilisateur ferme une session. UPHClean nettoie les handles de clé de registre pouvant être isolés par d'autres processus et applications. Ce service permet de s'assurer que la ruche de registre de l'utilisateur est déchargée pour qu'elle puisse être chargée correctement et que le persona local puisse être supprimé.

Si vous configurez Gestion de persona View sur des machines virtuelles Windows XP, téléchargez et installez UPHClean dans le système d'exploitation client.

Vous pouvez télécharger le service UPHClean à l'emplacement suivant : http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=6676.

Le service UPHClean est inclus avec les systèmes d'exploitation Windows 7 et Windows Vista. Vous n'avez pas à installer le service sur ces systèmes d'exploitation.

Installer View Persona Management autonome

Pour utiliser View Persona Management avec des ordinateurs physiques ou des machines virtuelles non View, installez la version autonome de View Persona Management.

Installez le logiciel View Persona Management autonome sur chaque machine virtuelle ou ordinateur individuel dans votre déploiement ciblé.

Prérequis

- Vérifiez que vous effectuez l'installation sur un ordinateur physique ou une machine virtuelle Windows 8, Windows 7, Windows Vista ou Windows XP SP3. View Persona Management ne fonctionne pas sur des serveurs Windows Server ou sur des serveurs Microsoft Terminal Server. Vérifiez que le système satisfait les exigences décrites dans la section XX.
- Vérifiez que vous pouvez ouvrir une session en tant qu'administrateur sur le système.
- Vérifiez que View Agent 5.*x* ou supérieur n'est pas installé sur l'ordinateur.
- Vérifiez que le service natif RTO Virtual Profiles 2.0 n'est pas installé sur la machine virtuelle.

Procédure

1. Téléchargez le fichier du programme d'installation View Persona Management autonome sur la page de produits VMware à l'adresse http://www.vmware.com/fr/products/.

   Le nom de fichier du programme d'installation est `VMware-personamanagement-y.y.y-xxxxxx.exe` ou `VMware-viewagent-x86_64-y.y.y-xxxxxx.exe`, où *y.y.y* est le numéro de version et *xxxxxx* le numéro de build.
2. Pour démarrer le programme d'installation, double-cliquez sur le fichier du programme d'installation.
3. Acceptez les termes de licence VMware.
4. Cliquez sur **[Installer]** .

   Par défaut, View Persona Management est installé dans le répertoire `C:\Program Files\VMware\VMware View Persona Management`.
5. Cliquez sur **[Terminer]** .
6. Redémarrez votre système pour que les modifications de l'installation prennent effet.

Suivant

Ajoutez le fichier de modèle d'administration de View Persona Management à votre configuration Active Directory ou de stratégie de groupe local.

Ajouter le fichier de modèle d'administration de View Persona Management (Gestion de Persona View)

Le fichier de modèle d'administration de View Persona Management (Gestion de Persona View) contient des paramètres de stratégie de groupe qui vous permettent de configurer Gestion de persona View. Pour pouvoir configurer les stratégies, vous devez ajouter le modèle de fichier ADM aux systèmes locaux ou au serveur Active Directory.

Pour configurer Gestion de persona View sur un seul système, vous pouvez ajouter les paramètres de stratégie de groupe à la configuration de stratégie d'ordinateur local sur ce système local.

Pour configurer Gestion de persona View pour un pool de postes de travail, vous pouvez ajouter les paramètres de stratégie de groupe à la configuration Stratégie Ordinateur local sur la machine virtuelle que vous utilisez en tant que parent ou modèle afin de déployer le pool de postes de travail.

Pour configurer Gestion de persona View au niveau domaine et appliquer la configuration à plusieurs postes de travail ou à l'ensemble de votre déploiement, vous pouvez ajouter les paramètres de stratégie de groupe à des objets de stratégie de groupe (GPO) sur votre serveur Active Directory. Dans Active Directory, vous pouvez créer une UO pour les postes de travail qui utilisent Gestion de persona View, créer un ou plusieurs GPO et lier les GPO à l'UO. Pour configurer des stratégies Gestion de persona View séparées pour différents types d'utilisateurs, vous pouvez créer des UO pour des ensembles particuliers de postes de travail et appliquer différents GPO aux UO.

Par exemple, vous pouvez créer une UO pour les postes de travail View avec Gestion de persona View et une autre UO pour les ordinateurs physiques sur lesquels le logiciel Gestion de persona View autonome est installé.

Pour voir un exemple d'implémentation de stratégie de groupe Active Directory dans View, reportez-vous à la section « Exemple de stratégie de groupe Active Directory », page 255.

Ajouter le modèle d'administration de Gestion de persona à un système unique

Pour configurer Gestion de persona View pour un pool de postes de travail unique, vous devez ajouter le fichier de modèle d'administration de Gestion de persona à la stratégie Ordinateur local sur la machine virtuelle que vous utilisez pour créer le pool. Pour configurer Gestion de persona View sur un système unique, vous devez ajouter le fichier de modèle d'administration de Gestion de persona à ce système.

Prérequis

- Vérifiez que View Agent est installé avec l'option d'installation de Gestion de persona View sur le système. Reportez-vous à la section « Installer View Agent avec l'option View Persona Management », page 268.
- Vérifiez que vous pouvez ouvrir une session en tant qu'administrateur sur le système.

Procédure

1 Sur le système local, cliquez sur **[Start (Démarrer)]** > **[Run (Exécuter)]** .

2 Saisissez **`gpedit.msc`** et cliquez sur **[OK]** .

3 Dans la fenêtre Local Computer Policy (Stratégie Ordinateur local), allez à **[Computer Configuration (Configuration ordinateur)]** et cliquez avec le bouton droit sur **[Administrative Templates (Modèles administratifs)]** .

Remarque Ne sélectionnez pas **[Administrative Templates (Modèles administratifs)]** sous **[User Configuration (Configuration utilisateur)]** .

---

4 Cliquez sur **[Add/Remove Templates (Ajout/Suppression de modèles)]** et cliquez sur **[Add (Ajouter)]** .

5 Accédez au répertoire qui contient le modèle de fichier ADM, `ViewPM.adm`.

Type d'installation	Directory
View Agent avec l'option d'installation [Gestion de persona View]	*install_directory*\VMware\VMware View\Agent\bin Le fichier `ViewPM.adm` est également installé avec les autres fichiers de modèle d'administration de View dans le répertoire *install_directory*\VMware\VMware View\Server\extras\GroupPolicyFiles sur l'hôte de Serveur de connexion View.
Gestion de persona View autonome	*install_directory*\VMware\VMware Gestion de persona View

6 Sélectionnez le fichier `ViewPM.adm` et cliquez sur **[Add (Ajouter)]** .

7 Fermer la fenêtre Add/Remove Templates (Ajout/Suppression de modèles).

Les paramètres de stratégie de groupe de Gestion de persona View sont ajoutés à la configuration Stratégie Ordinateur local sur le système local. Vous devez utiliser `gpedit.msc` pour afficher cette configuration.

Suivant

Configurez les paramètres de stratégie de groupe de Gestion de persona View sur le système local. Reportez-vous à la section « Configurer des stratégies View Persona Management (Gestion de Persona View) », page 273.

Ajouter le modèle d'administration de Gestion de persona à Active Directory

Pour configurer Gestion de persona View pour votre déploiement, vous pouvez ajouter le fichier de modèle d'administration de Gestion de persona à un objet de stratégie de groupe (GPO) dans votre serveur Active Directory.

Prérequis

- Créez des GPO pour votre déploiement de Gestion de persona View et liez-les à l'UO contenant les postes de travail View qui utilisent Gestion de persona View. Reportez-vous à la section « Exemple de stratégie de groupe Active Directory », page 255.
- Vérifiez que les composants logiciels enfichables Microsoft MMC et que l'Éditeur d'objets de stratégie de groupe sont disponibles sur votre serveur Active Directory.
- Vérifiez que View Agent est installé avec l'option d'installation de Gestion de persona View sur un système accessible à votre serveur Active Directory. Reportez-vous à la section « Installer View Agent avec l'option View Persona Management », page 268.

Procédure

1 Copiez le fichier de modèle d'administration de Gestion de persona View, `ViewPM.adm`, sur votre serveur Active Directory.

Le fichier `ViewPM.adm` est situé dans le répertoire *install_directory*\VMware\VMware View\Server\extras\GroupPolicyFiles sur l'hôte de Serveur de connexion View.

Si Gestion de persona View autonome est installé sur un système non-View, le fichier `ViewPM.adm` se trouve dans le répertoire *install_directory*\VMware\VMware Gestion de persona View.

2 Sur votre serveur Active Directory, ouvrez la Console de gestion des stratégies de groupe.

Par exemple, ouvrez la boîte de dialogue Run (Exécuter), tapez **`gpmc.msc`** et cliquez sur **[OK]** .

3 Dans le volet de gauche, sélectionnez le domaine ou l'UO contenant vos postes de travail View.

4 Dans le volet de droite, cliquez avec le bouton droit sur le GPO que vous avez créé pour les paramètres de stratégie de groupe et sélectionnez **[Edit (Modifier)]** .

La fenêtre Group Policy Object Editor (Éditeur d'objets de stratégie de groupe) apparaît.

5 Dans l'Éditeur d'objets de stratégie de groupe, cliquez avec le bouton droit sur **[Administrative Templates (Modèles administratifs)]** sous **[Computer Configuration (Configuration ordinateur)]** et sélectionnez **[Add/Remove Templates (Ajout/Suppression de modèles)]** .

6 Cliquez sur **[Add (Ajouter)]** , recherchez le fichier `ViewPM.adm` et cliquez sur **[Open (Ouvrir)]** .

7 Cliquez sur **[Close (Fermer)]** pour appliquer les paramètres de stratégie dans le fichier de modèle d'administration au GPO.

Le nom du modèle apparaît dans le volet gauche sous **[Administrative Templates (Modèles administratifs)]** .

Suivant

Configurez les paramètres de stratégie de groupe de Gestion de persona View sur votre serveur Active Directory.

Configurer des stratégies View Persona Management (Gestion de Persona View)

Pour utiliser Gestion de persona View, vous devez activer le paramètre de stratégie de groupe **[Manage user persona (Gérer un persona d'utilisateur)]** , ce qui active le logiciel Gestion de persona View. Pour configurer un référentiel de profils d'utilisateur sans utiliser de chemin de profil d'utilisateur Active Directory, vous devez configurer le paramètre de stratégie de groupe **[Persona repository location (Emplacement du référentiel de persona)]** .

Vous pouvez configurer les paramètres de stratégie de groupe facultatifs pour configurer d'autres aspects de votre déploiement de Gestion de persona View.

Si des profils itinérants de Windows sont déjà configurés dans votre déploiement, vous pouvez utiliser un chemin de profil d'utilisateur Active Directory existant. Vous pouvez laisser le paramètre **[Persona repository location (Emplacement du référentiel de persona)]** désactivé ou non configuré.

Prérequis

- Familiarisez-vous avec les paramètres de stratégie de groupe **[Manage user persona (Gérer un persona d'utilisateur)]** et **[Persona repository location (Emplacement du référentiel de persona)]** . Reportez-vous à la section « Paramètres de stratégie de groupe d'itinérance et de synchronisation », page 281.
- Si vous configurez des stratégies de groupe sur un système local, familiarisez-vous avec l'ouverture de la fenêtre Group Policy (Stratégie de groupe). Reportez-vous aux étapes Étape 1 et Étape 2 de la section « Ajouter le modèle d'administration de Gestion de persona à un système unique », page 271.
- Si vous configurez des stratégies de groupe sur votre serveur Active Directory, familiarisez-vous avec le démarrage de l'Éditeur d'objets de stratégie de groupe. Reportez-vous aux étapes Étape 2 à Étape 4 de la section « Ajouter le modèle d'administration de Gestion de persona à Active Directory », page 272.

Procédure

1 Ouvrez la fenêtre Group Policy (Stratégie de groupe).

Option	Description
Local system (Système local)	Ouvrez la fenêtre Local Computer Policy (Stratégie Ordinateur local).
Active Directory server (Serveur Active Directory)	Ouvrez la fenêtre Group Policy Object Editor (Éditeur d'objets de stratégie de groupe).

2 Développez le dossier **[Computer Configuration (Configuration ordinateur)]** et allez dans le dossier **[Persona Management (Gestion de persona)]** .

Option	Description
Windows XP ou Windows Server 2003	Développez les dossiers suivants : **[Administrative Templates (Modèles administratifs)]** , **[VMware View Agent Configuration (Configuration de VMware View Agent)]** , **[Persona Management (Gestion de persona)]**
Windows Vista et supérieur ou Windows Server 2008 et supérieur	Développez les dossiers suivants : **[Administrative Templates (Modèles administratifs)]** , **[Classic Administrative Templates (ADM) (Modèles d'administration classiques)]** , **[VMware View Agent Configuration (Configuration de VMware View Agent)]** , **[Persona Management (Gestion de persona)]**

3 Ouvrez le dossier **[Roaming & Synchronization (Itinérance et synchronisation)]** .

4 Double-cliquez sur **[Manage user persona (Gérer un persona d'utilisateur)]** et cliquez sur **[Enabled (Activé)]** .

Ce paramètre active View Persona Management (Gestion de Persona View). Lorsque)ce paramètre est désactivé ou n'est pas configuré, View Persona Management (Gestion de persona View) ne fonctionne pas.

5 Saisissez l'intervalle de chargement du profil, en minutes, et cliquez sur **[OK]** .

L'intervalle de chargement du profil détermine la fréquence à laquelle (Gestion de persona View) copie des modifications de profil d'utilisateur dans le référentiel distant. L'intervalle de chargement par défaut est 10 minutes.

6 Double-cliquez sur **[Persona repository location (Emplacement du référentiel de persona)]** et cliquez sur **[Enabled (Activé)]** .

Si vous possédez un déploiement de profils itinérants de Windows existant, vous pouvez utiliser un chemin de profil d'utilisateur Active Directory pour le référentiel de profils distant. Vous n'avez pas à configurer un **[Persona repository location (Emplacement du référentiel de persona)]** .

7 Saisissez le chemin d'accès UNC vers un partage de serveur de fichiers de réseau qui stocke les profils d'utilisateur.

Par exemple : `\\server.domain.com\UserProfilesRepository\%username%`

Le partage de réseau doit être accessible pour les machines virtuelles dans votre déploiement.

Si vous prévoyez d'utiliser un chemin de profil d'utilisateur Active Directory, vous n'avez pas à spécifier un chemin d'accès UNC.

8 Si un chemin de profil d'utilisateur Active Directory est configuré dans votre déploiement, déterminez si vous voulez utiliser ou remplacer ce chemin.

Option	Action
Utiliser le partage de réseau.	Cochez la case **[Override Active Directory user profile path if it is configured (Remplacer le chemin de profil d'utilisateur Active Directory s'il est configuré)]** .
Utiliser un chemin de profil d'utilisateur Active Directory, s'il en existe un.	Ne cochez pas la case **[Override Active Directory user profile path if it is configured (Remplacer le chemin de profil d'utilisateur Active Directory s'il est configuré)]** .

9 Cliquez sur **[OK]** .

10 (Facultatif) Configurez d'autres paramètres de stratégie de groupe View Persona Management (Gestion de Persona View).

Créer des postes de travail View qui utilisent Gestion de persona

Pour utiliser Gestion de persona View avec des postes de travail View, vous devez créer des pools de postes de travail avec un agent Gestion de persona View installé sur chaque poste de travail.

Vous ne pouvez pas utiliser Gestion de persona View sur des serveurs Microsoft Terminal Server.

Vous ne pouvez pas utiliser View Persona Management (Gestion de Persona View) avec des postes de travail exécutés en mode local.

Prérequis

- Vérifiez que View Agent avec l'option d'installation **[View Persona Management (Gestion de persona View)]** est installé sur la machine virtuelle que vous utilisez pour créer le pool de postes de travail. Reportez-vous à la section « Installer View Agent avec l'option View Persona Management », page 268.
- Si vous prévoyez de configurer des stratégies de Gestion de persona View pour ce pool uniquement, vérifiez que vous avez ajouté le fichier de modèle d'administration de Gestion de persona View à la machine virtuelle et configuré des paramètres de stratégie de groupe dans la configuration Stratégie Ordinateur local. Reportez-vous aux sections « Ajouter le modèle d'administration de Gestion de persona à un système unique », page 271 et« Configurer des stratégies View Persona Management (Gestion de Persona View) », page 273.

Procédure

- Générez un snapshot ou un modèle depuis la machine virtuelle et créez un pool de postes de travail automatisé.

  Vous pouvez configurer Gestion de persona View avec des pools qui contiennent des machines virtuelles complètes ou des clones liés. Les pools peuvent utiliser des affectations dédiées ou flottantes.
- (Facultatif) Pour utiliser Gestion de persona View avec des pools de postes de travail manuels, sélectionnez des sources de postes de travail sur lesquelles View Agent avec l'option **[View Persona Management (Gestion de persona View)]** est installé.

Remarque Une fois que vous avez déployé Gestion de persona View sur vos postes de travail View, si vous supprimez l'option d'installation **[View Persona Management (Gestion de persona View)]** sur les postes de travail, ou si vous désinstallez View Agent complètement, les profils d'utilisateur locaux sont supprimés des postes de travail des utilisateurs qui n'ont actuellement pas de session ouverte. Pour les utilisateurs dont une session est actuellement ouverte, les profils d'utilisateur sont téléchargés à partir du référentiel de profils distant lors du processus de désinstallation.

Meilleures pratiques pour la configuration d'un déploiement de gestion de persona View

Vous devez suivre des meilleures pratiques pour la configuration de gestion de persona View afin d'accroître l'expérience de vos utilisateurs sur les postes de travail, améliorer les performances du poste de travail et vous assurer que Gestion de persona View fonctionne efficacement avec d'autres fonctions de View.

Choisir de supprimer des profils d'utilisateur locaux à la fermeture de session

Par défaut, Gestion de persona View ne supprime pas les profils d'utilisateur des postes de travail locaux lorsque des utilisateurs ferment une session. La stratégie **[Remove local persona at log off (Supprimer le persona local à la fermeture de session)]** est désactivée. Dans de nombreux cas, le paramètre par défaut est une meilleure pratique car il réduit les opérations d'E/S et évite le comportement redondant.

Par exemple, laissez cette stratégie désactivée si vous déployez des pools d'affectation flottante, puis actualisez ou supprimez les postes de travail à la fermeture de session. Le profil local est supprimé lorsque la machine virtuelle est actualisée ou supprimée. Dans un pool automatisé d'affectation flottante, des machines virtuelles complètes peuvent être supprimées après la fermeture de session. Dans un pool de clone lié d'affectation flottante, les clones peuvent être actualisés ou supprimés à la fermeture de session.

Si vous déployez des pools d'affectation dédiée, vous pouvez laisser la stratégie désactivée car les utilisateurs reviennent aux mêmes postes de travail à chaque session. Avec la stratégie désactivée, lorsqu'un utilisateur ouvre une session, Gestion de persona View n'a pas à télécharger les fichiers présents dans le profil local. Si vous configurez des pools de clone lié d'affectation dédiée avec des disques persistants, laissez la stratégie désactivée pour éviter de supprimer des données d'utilisateur des disques persistants.

Dans certains cas, vous voulez peut-être activer la stratégie **[Remove local persona at log off (Supprimer le persona local à la fermeture de session)]** .

Gestion des déploiements incluant Gestion de persona View et des profils itinérants de Windows

Dans des déploiements dans lesquels des profils itinérants de Windows sont configurés, et où les utilisateurs accèdent à des postes de travail View avec Gestion de persona View et à des postes de travail standard avec des profils itinérants de Windows, la meilleure pratique consiste à utiliser des profils différents pour les deux environnements de postes de travail. Si un poste de travail View et l'ordinateur client à partir duquel le poste de travail est lancé se trouvent dans le même domaine, et si vous utilisez un GPO Active Directory pour configurer à la fois des profils itinérants de Windows et Gestion de persona View, activez la stratégie **[Persona repository location (Emplacement du référentiel de persona)]** et sélectionnez **[Override Active Directory user profile path if it is configured (Remplacer le chemin de profil d'utilisateur Active Directory s'il est configuré)]** .

Cette approche évite à des profils itinérants de Windows de remplacer un profil Gestion de persona View lorsque l'utilisateur ferme une session sur l'ordinateur client.

Si des utilisateurs prévoient de partager des données entre des profils itinérants de Windows existants et des profils Gestion de persona View, vous pouvez configurer la redirection de dossiers Windows.

Configuration de chemins d'accès pour des dossiers redirigés

Lorsque vous utilisez le paramètre de stratégie de groupe **[Folder Redirection (Redirection de dossiers)]** , configurez le chemin de dossier pour inclure `%username%`, mais assurez-vous que le dernier sous-dossier dans le chemin utilise le nom du dossier redirigé, tel que `My Videos`. Le dernier dossier dans le chemin est affiché sous la forme du nom de dossier sur le poste de travail de l'utilisateur.

Par exemple, si vous configurez un chemin tel que `\\myserver\videos\%username%\My Videos`, le nom de dossier qui apparaît sur le poste de travail de l'utilisateur est `My Videos`.

Si `%username%` est le dernier sous-dossier dans le chemin, le nom de l'utilisateur apparaît sous la forme du nom de dossier. Par exemple, au lieu de voir un dossier `My Videos` sur le poste de travail, l'utilisateur `JDoe` voit un dossier avec le nom `JDoe` et ne peut pas identifier facilement le dossier.

Meilleures pratiques supplémentaires

Vous pouvez également suivre ces recommandations :

- Par défaut, de nombreux antivirus n'analysent pas les fichiers hors ligne. Par exemple, lorsqu'un utilisateur ouvre une session sur un poste de travail, ces antivirus n'analysent pas les fichiers de profil d'utilisateur qui ne sont pas spécifiés dans le paramètre de stratégie de groupe **[Files and folders to preload (Fichiers et dossiers à précharger)]** ou **[Windows roaming profiles synchronization (Synchronisation de profils itinérants de Windows)]** . Pour de nombreux déploiements, le comportement par défaut est la meilleure pratique car elle réduit l'E/S requise pour télécharger des fichiers lors d'analyses à la demande.

  Si vous voulez récupérer des fichiers du référentiel distant et activer l'analyse des fichiers hors ligne, consultez la documentation de votre antivirus.

- Il vous est fortement recommandé d'utiliser des pratiques standard pour sauvegarder des partages réseau sur lesquels Gestion de persona View stocke le référentiel de profils.

  Remarque N'utilisez pas de logiciel de sauvegarde tel que MozyPro ou les services de sauvegarde Windows Volume avec Gestion de persona View pour sauvegarder des profils d'utilisateur sur des postes de travail View.

  Gestion de persona View s'assure que les profils d'utilisateur sont sauvegardés sur le référentiel de profils distant, ce qui évite d'utiliser des outils supplémentaires pour sauvegarder les données d'utilisateur sur les postes de travail. Dans certains cas, des outils tels que MozyPro ou les services de sauvegarde Windows Volume peuvent interférer avec Gestion de persona View et entraîner la perte ou la corruption de données.

- Vous pouvez définir des stratégies Gestion de persona View pour améliorer les performances lorsque des utilisateurs démarrent des applications ThinApp. Reportez-vous à la section « Configuration de profils d'utilisateur pour inclure des dossiers de sandbox ThinApp », page 277.

- Si vos utilisateurs génèrent des données de persona substantielles, et si vous prévoyez d'utiliser l'actualisation et la recomposition pour gérer des postes de travail de clone lié d'affectation dédiée, configurez votre pool de postes de travail afin d'utiliser des disques persistants de View Composer séparés. Les disques persistants peuvent améliorer les performances de Gestion de persona View. Reportez-vous à la section « Configuration de disques persistants de View Composer avec View Persona Management », page 278.

- Si vous configurez Gestion de persona View pour des ordinateurs portables autonomes, veillez à maintenir les profils synchronisés lorsque les utilisateurs passent hors ligne. Reportez-vous à la section « Gérer les profils d'utilisateur sur les ordinateurs portables autonomes », page 278.

Configuration de profils d'utilisateur pour inclure des dossiers de sandbox ThinApp

View Persona Management conserve les paramètres d'utilisateur associés à des applications ThinApp en incluant des dossiers de sandbox ThinApp dans les profils d'utilisateur. Vous pouvez définir des stratégies View Persona Management pour améliorer les performances lorsque des utilisateurs démarrent des applications ThinApp.

View Persona Management précharge des dossiers et des fichiers de sandbox ThinApp dans le profil d'utilisateur local lorsqu'un utilisateur ouvre une session. Les dossiers de sandbox ThinApp sont créés avant qu'un utilisateur puisse terminer l'ouverture de session. Pour améliorer les performances, View Persona Management ne télécharge pas les données de sandbox ThinApp lors de l'ouverture de session, bien que les fichiers soient créés sur le poste de travail local avec les mêmes attributs et tailles de base que les fichiers de sandbox ThinApp dans le profil distant de l'utilisateur.

Comme meilleure pratique, il vous est conseillé de télécharger les données de sandbox ThinApp réelles en arrière-plan. Activez le paramètre de stratégie de groupe **[Folders to background download (Dossiers à télécharger en arrière-plan)]** et ajoutez les dossiers de sandbox ThinApp. Reportez-vous à la section « Paramètres de stratégie de groupe d'itinérance et de synchronisation », page 281.

Les fichiers de sandbox ThinApp réels peuvent être volumineux. Avec le paramètre **[Folders to background download (Dossiers à télécharger en arrière-plan)]** , les utilisateurs n'ont pas à attendre que des fichiers volumineux se téléchargent lorsqu'ils démarrent une application. De plus, les utilisateurs n'ont pas à attendre que les fichiers se préchargent lorsqu'ils ouvrent une session, comme ils le devraient si vous utilisez le paramètre **[Files and folders to preload (Fichiers et dossiers à précharger)]** avec des fichiers volumineux.

Configuration de disques persistants de View Composer avec View Persona Management

Avec des disques persistants de View Composer, vous pouvez conserver des données et des paramètres d'utilisateur tout en gérant des disques du système d'exploitation de clone lié avec des opérations d'actualisation, de recomposition et de rééquilibrage. La configuration de disques persistants peut améliorer les performances de View Persona Management lorsque les utilisateurs génèrent une grande quantité d'informations de persona. Vous pouvez configurer des disques persistants uniquement avec des postes de travail de clone lié d'affectation dédiée.

View Persona Management conserve chaque profil d'utilisateur sur un référentiel distant configuré sur un partage de réseau. Une fois qu'un utilisateur ouvre une session sur un poste de travail, les fichiers de persona sont téléchargés dynamiquement lorsque l'utilisateur en a besoin.

Si vous configurez des disques persistants avec View Persona Management, vous pouvez actualiser et recomposer les disques du système d'exploitation de clone lié et conserver une copie locale de chaque profil d'utilisateur sur les disques persistants.

Les disques persistants peuvent agir comme un cache pour les profils d'utilisateur. Lorsqu'un utilisateur requiert des fichiers de persona, View Persona Management n'a pas besoin de télécharger les données qui sont les mêmes sur le disque persistant local et sur le référentiel distant. Seules les données de persona non synchronisées doivent être téléchargées.

Si vous configurez des disques persistants, n'activez pas la stratégie **[Remove local persona at log off (Supprimer le persona local à la fermeture de session)]** . L'activation de cette stratégie supprime les données d'utilisateur des disques persistants lorsque des utilisateurs ferment une session.

Gérer les profils d'utilisateur sur les ordinateurs portables autonomes

Si vous installez Gestion de persona View sur des ordinateurs portables autonomes (non-View), veillez à maintenir les profils d'utilisateur synchronisés lorsque les utilisateurs mettent leurs ordinateurs portables autonomes hors ligne.

Pour que l'ordinateur portable autonome d'un utilisateur ait un profil local à jour, vous pouvez configurer le paramètre de stratégie de groupe Gestion de persona View `Enable background download for laptops`. Ce paramètre télécharge l'ensemble du profil d'utilisateur vers l'ordinateur portable autonome en arrière-plan.

Comme meilleure pratique, notifiez les utilisateurs pour que leurs profils d'utilisateur soient complètement téléchargés avant qu'ils se déconnectent du réseau. Demandez aux utilisateurs d'attendre l'affichage de l'avis `Background download complete` sur leur écran avant de se déconnecter.

Pour afficher l'avis `Background download complete` sur les ordinateurs portables des utilisateurs, définissez le paramètre de stratégie de groupe Gestion de persona View, `Show critical errors to users via tray icon alerts`.

Si l'utilisateur se déconnecte du réseau avant la fin du téléchargement de profil, le profil local et le profil distant risquent de ne plus être synchronisés. Lorsque l'utilisateur est hors ligne, il pourrait mettre à jour un fichier local qui n'a pas été complètement téléchargé. Lorsque l'utilisateur se reconnecte au réseau, le profil local est envoyé en remplaçant le profil distant. Les données qui se trouvaient dans le profil distant d'origine sont perdues.

Voici un exemple d'étapes à suivre.

Prérequis

Vérifiez que Gestion de persona View est configuré pour les ordinateurs portables autonomes des utilisateurs. Reportez-vous à la section « Configuration d'un déploiement de Gestion de Persona View », page 266.

Procédure

1 Dans l'UO Active Directory qui contrôle les ordinateurs portables autonomes, activez le paramètre `Enable background download for laptops`.

Dans l'éditeur d'objet de stratégie de groupe, développez les dossiers suivants : **[Computer Configuration (Configuration ordinateur)]**, **[Administrative Templates (Modèles administratifs)]**, **[Classic Administrative Templates (ADM) (Modèles d'administration classiques)]** > **[VMware View Agent Configuration (Configuration de VMware View Agent)]** > **[Persona Management (Gestion de persona)]**, **[Roaming & Synchronization (Itinérance et synchronisation)]**

Le dossier **[Classic Administrative Templates (ADM) (Modèles d'administration classiques)]** apparaît uniquement dans Windows Vista et les versions suivantes et Windows Server 2008 et les versions suivantes.

2 Pour les ordinateurs portables autonomes, vous devez utiliser une méthode non-View pour notifier les utilisateurs lorsqu'ils ouvrent une session.

Par exemple, vous pouvez diffuser le message suivant :
`Vos données personnelles sont téléchargées dynamiquement vers votre ordinateur portable après l'ouverture d'une session. Attendez la fin du téléchargement de vos données personnelles avant de déconnecter votre ordinateur portable du réseau. Un avis de fin de téléchargement en arrière-plan s'affichera lorsque le téléchargement de vos données personnelles sera terminé.`

Paramètres de stratégie de groupe Gestion de persona View

Le fichier de modèle d'administration de Gestion de persona View contient des paramètres de stratégie de groupe que vous ajoutez à la configuration Stratégie de groupe sur des systèmes individuels ou sur un serveur Active Directory. Vous devez configurer les paramètres de stratégie de groupe pour configurer et contrôler plusieurs aspects de Gestion de persona View.

Le fichier de modèle d'administration, `ViewPM.adm`, est installé avec les autres fichiers de modèle d'administration de View dans le répertoire *`install_directory`*`\VMware\VMware View\Server\extras\GroupPolicyFiles` sur l'hôte de Serveur de connexion View.

Lorsque vous installez View Agent avec l'option d'installation **[View Persona Management (Gestion de persona View)]**, le fichier `ViewPM.adm` est également installé sur la machine virtuelle dans le répertoire *`install_directory`*`\VMware\VMware View\Agent\bin`.

Lorsque vous installez Gestion de persona autonome sur un système non-View, le fichier `ViewPM.adm` se trouve sur le système dans le répertoire *`install_directory`*`\VMware\VMware Gestion de persona View`.

Une fois que vous avez ajouté le fichier `ViewPM.adm` à votre configuration Stratégie de groupe, les paramètres de règle se trouvent dans le dossier **[Persona Management (Gestion de persona)]** dans la fenêtre Group Policy (Stratégie de groupe).

Tableau 9-2. Emplacement des paramètres de Gestion de persona View dans la fenêtre Group Policy (Stratégie de groupe)

Système d'exploitation	Emplacement
Windows Vista et supérieur ou Windows Server 2008 et supérieur	**[Computer Configuration (Configuration ordinateur)]** > **[Administrative Templates (Modèles administratifs)]** > **[Classic Administrative Templates (ADM) (Modèles d'administration classiques)]** > **[VMware View Agent Configuration (Configuration de VMware View Agent)]** > **[Gestion de persona]**
Windows XP ou Windows Server 2003	**[Computer Configuration (Configuration ordinateur)]** > **[Administrative Templates (Modèles administratifs)]** > **[VMware View Agent Configuration (Configuration de VMware View Agent)]** > **[Gestion de persona]**

Les paramètres de stratégie de groupe sont contenus dans ces dossiers :

- Roaming & Synchronization (Itinérance et synchronisation)
- Folder Redirection (Redirection de dossiers)
- Desktop UI (Interface utilisateur de poste de travail)
- Logging (Journalisation)

Paramètres de stratégie de groupe d'itinérance et de synchronisation

Les paramètres de stratégie de groupe d'itinérance et de synchronisation activent et désactivent View Persona Management, définissent l'emplacement du référentiel de profils distant, déterminent quels dossiers et quels fichiers appartiennent au profil d'utilisateurs, et contrôlent la façon dont sont synchronisés les dossiers et les fichiers.

Paramètre de stratégie de groupe	Description
Gérer un persona d'utilisateur	Détermine si vous voulez gérer des profils d'utilisateur dynamiquement avec View Persona Management ou avec des profils itinérants de Windows. Ce paramètre active et désactive View Persona Management. Lorsque ce paramètre est activé, View Persona Management gère des profils d'utilisateur. Lorsque le paramètre est activé, vous pouvez spécifier un intervalle de chargement du profil en minutes. Cette valeur détermine la fréquence de copie des modifications du profil d'utilisateur dans le référentiel distant. La valeur par défaut est 10 minutes. Lorsque ce paramètre est désactivé ou n'est pas configuré, les profils d'utilisateur sont gérés par Windows.
Emplacement du référentiel de persona	Spécifie l'emplacement du référentiel de profils d'utilisateur. Ce paramètre détermine également si vous voulez utiliser un partage de réseau spécifié dans View Persona Management ou un chemin d'accès configuré dans Active Directory afin de prendre en charge des profils itinérants de Windows. Lorsque ce paramètre est activé, vous pouvez utiliser le **[Chemin de partage]** pour déterminer l'emplacement du référentiel de profils d'utilisateur. Dans la zone de texte **[Chemin de partage]** , vous spécifiez un chemin d'accès UNC vers un partage de réseau accessible aux postes de travail View Persona Management. Ce paramètre permet à View Persona Management de contrôler l'emplacement du référentiel de profils d'utilisateur. Par exemple : `\\server.domain.com\VPRepository` Si `%username%` ne fait pas partie du chemin de dossier que vous configurez, View Persona Management ajoute `%username%.%userdomain%` au chemin. Par exemple : `\\server.domain.com\VPRepository\%username%.%userdomain%` Si vous spécifiez un emplacement dans **[Chemin de partage]** , vous n'avez pas à régler des profils itinérants dans Windows ou à configurer un chemin de profil d'utilisateur dans Active Directory pour prendre en charge des profils itinérants de Windows. Pour plus d'informations sur la configuration d'un partage de réseau UNC pour View Persona Management, reportez-vous à la section « Configurer un référentiel de profils d'utilisateur », page 267. Par défaut, le chemin de profil d'utilisateur Active Directory est utilisé. En particulier, lorsque **[Chemin de partage]** est laissé vide, le chemin de profil d'utilisateur Active Directory est utilisé. Le **[Chemin de partage]** est vide et inactif lorsque ce paramètre est désactivé ou n'est pas configuré. Vous pouvez également laisser le chemin vide lorsque ce paramètre est activé. Lorsque ce paramètre est activé, vous pouvez cocher la case **[Remplacer le chemin de profil d'utilisateur Active Directory s'il est configuré]** pour vous assurer que View Persona Management utilise le chemin spécifié dans **[Chemin de partage]** . Par défaut, cette case est décochée, et View Persona Management utilise le chemin de profil d'utilisateur Active Directory lorsque les deux emplacements sont configurés.
Supprimer le persona local à la fermeture de session	Supprime le profil stocké localement de chaque utilisateur du système de poste de travail lorsque l'utilisateur ferme une session. Vous pouvez également cocher une case pour supprimer les dossiers de paramètres locaux de chaque utilisateur lorsque le profil d'utilisateur est supprimé. Lorsque vous utilisez Windows 8, Windows 7 ou Windows Vista, cocher cette case supprime le dossier `AppData\Local`. Dans Windows XP, cocher cette case supprime le dossier `Paramètres locaux`. Pour voir des recommandations sur l'utilisation de ce paramètre, reportez-vous à la section « Meilleures pratiques pour la configuration d'un déploiement de gestion de persona View », page 275. Lorsque ce paramètre est désactivé ou n'est pas configuré, les profils d'utilisateur stockés localement, y compris les dossiers de paramètres locaux, ne sont pas supprimés lorsque les utilisateurs ferment une session.

Paramètre de stratégie de groupe	Description
Déplacer des dossiers de paramètres locaux	Déplace les dossiers de paramètres locaux avec le reste de chaque profil d'utilisateur. Pour Windows 8, Windows 7 ou Windows Vista, cette stratégie affecte le dossier `AppData\Local`. Pour Windows XP, cette stratégie affecte le dossier `Paramètres locaux`. Par défaut, les paramètres locaux ne sont pas déplacés.
Fichiers et dossiers à précharger	Spécifie une liste de fichiers et de dossiers téléchargés vers le profil d'utilisateur local quand l'utilisateur ouvre une session. Les modifications dans les fichiers sont copiées sur le référentiel distant au moment où elles se produisent. Dans certaines situations, vous voulez peut-être précharger des fichiers et des dossiers spécifiques dans le profil d'utilisateur stocké localement. Utilisez ce paramètre pour spécifier ces fichiers et dossiers. Spécifiez des chemins liés à la racine du profil local. Ne spécifiez pas de lecteur dans un nom de chemin d'accès. Par exemple : `Application Data\Microsoft\Certificates` Après le préchargement des fichiers et des dossiers spécifiés, View Persona Management gère les fichiers et les dossiers comme il gère d'autres données de profil. Lorsqu'un utilisateur met à jour des fichiers et des dossiers préchargés, View Persona Management copie les données mises à jour vers le référentiel de profils distant au cours de la session, au prochain intervalle de chargement du profil.
Fichiers et dossiers à précharger (exceptions)	Empêche le préchargement des fichiers et des dossiers spécifiés. Les chemins de dossier sélectionnés doivent résider dans les dossiers que vous spécifiez dans le paramètre **[Fichiers et dossiers à précharger]** . Spécifiez des chemins liés à la racine du profil local. Ne spécifiez pas de lecteur dans un nom de chemin d'accès.
Synchronisation de profils itinérants de Windows	Spécifie une liste de fichiers et de dossiers gérés par des profils itinérants de Windows standard. Les fichiers et les dossiers sont récupérés depuis le référentiel distant quand l'utilisateur ouvre une session. Les fichiers ne sont pas copiés sur le référentiel distant jusqu'à ce que l'utilisateur ferme une session. Pour les fichiers et les dossiers spécifiés, View Persona Management ignore l'intervalle de réplication des profils configuré par le **[Intervalle de chargement du profil]** dans le paramètre **[Gérer un persona d'utilisateur]** . Spécifiez des chemins liés à la racine du profil local. Ne spécifiez pas de lecteur dans un nom de chemin d'accès.
Synchronisation de profils itinérants de Windows (exceptions)	Les fichiers et les dossiers sélectionnés sont des exceptions aux chemins spécifiés dans le paramètre **[Synchronisation de profils itinérants de Windows]** . Les chemins de dossier sélectionnés doivent résider dans les dossiers que vous spécifiez dans le paramètre **[Synchronisation de profils itinérants de Windows]** . Spécifiez des chemins liés à la racine du profil local. Ne spécifiez pas de lecteur dans un nom de chemin d'accès.
Fichiers et dossiers exclus du déplacement	Spécifie une liste de fichiers et de dossiers qui ne sont pas déplacés avec le reste du profil d'utilisateur. Les fichiers et les dossiers spécifiés n'existent que sur le système local. Certaines situations requièrent que des fichiers et des dossiers spécifiques résident uniquement dans le profil d'utilisateur stocké localement. Par exemple, vous pouvez exclure les fichiers temporaires et mis en cache du déplacement. Ces fichiers n'ont pas à être répliqués dans le référentiel distant. Spécifiez des chemins liés à la racine du profil local. Ne spécifiez pas de lecteur dans un nom de chemin d'accès. Par défaut, le dossier temp du profil d'utilisateur, le dossier du cache d'application ThinApp et les dossiers du cache pour Internet Explorer, Firefox, Chrome et Opera sont exclus du déplacement.
Fichiers et dossiers exclus du déplacement (exceptions)	Les fichiers et les dossiers sélectionnés sont des exceptions aux chemins spécifiés dans le paramètre **[Fichiers et dossiers exclus du déplacement]** . Les chemins de dossier sélectionnés doivent résider dans les dossiers que vous spécifiez dans le paramètre **[Fichiers et dossiers exclus du déplacement]** . Spécifiez des chemins liés à la racine du profil local. Ne spécifiez pas de lecteur dans un nom de chemin d'accès.

Paramètre de stratégie de groupe	Description
Activer le téléchargement en arrière-plan pour les ordinateurs portables	Télécharge tous les fichiers dans le profil d'utilisateur lorsqu'un utilisateur ouvre une session sur un ordinateur portable sur lequel le logiciel View Persona Management est installé. Les fichiers sont téléchargés en arrière-plan. Lorsque l'opération est terminée, une notification contextuelle apparaît sur l'écran de l'utilisateur : `Téléchargement en arrière-plan terminé`. Pour autoriser cette notification à apparaître sur l'ordinateur portable de l'utilisateur, vous devez activer le paramètre `Afficher des erreurs critiques aux utilisateurs via des alertes d'icône de la barre d'état`. **Remarque** Si vous activez ce paramètre, il vous est recommandé d'en informer vos utilisateurs pour s'assurer que le profil est complètement téléchargé avant que les utilisateurs se déconnectent du réseau. Si un utilisateur met un ordinateur portable autonome hors ligne avant la fin du téléchargement de profil, l'utilisateur peut ne pas avoir accès aux fichiers de profils locaux. Lorsque l'utilisateur est hors ligne, il ne peut pas ouvrir un fichier local qui n'a pas été complètement téléchargé. Reportez-vous à la section « Gérer les profils d'utilisateur sur les ordinateurs portables autonomes », page 278.
Dossiers à télécharger en arrière-plan	Les dossiers sélectionnés sont téléchargés dans l'arrière-plan lorsqu'un utilisateur ouvre une session sur le poste de travail. Dans certains cas, vous pouvez optimiser View Persona Management en téléchargeant le contenu de dossiers spécifiques dans l'arrière-plan. Avec ce paramètre, les utilisateurs n'ont pas à attendre que des fichiers volumineux se téléchargent lorsqu'ils démarrent une application. De plus, les utilisateurs n'ont pas à attendre que les fichiers se préchargent lorsqu'ils ouvrent une session, comme ils le devraient si vous utilisez le paramètre **[Fichiers et dossiers à précharger]** avec des fichiers très volumineux. Par exemple, vous pouvez inclure des dossiers de sandbox ThinApp de VMware dans le paramètre **[Dossiers à télécharger en arrière-plan]** . Le téléchargement en arrière-plan n'affecte pas les performances lorsqu'un utilisateur ouvre une session ou utilise d'autres applications sur le poste de travail. Lorsque l'utilisateur démarre l'application ThinApp, les fichiers de sandbox ThinApp requis sont susceptibles d'être téléchargés depuis le référentiel distant, ce qui améliore l'heure de démarrage de l'application. Spécifiez des chemins liés à la racine du profil local. Ne spécifiez pas de lecteur dans un nom de chemin d'accès.
Dossiers à télécharger en arrière-plan (exceptions)	Les dossiers sélectionnés sont des exceptions aux chemins spécifiés dans le paramètre **[Dossiers à télécharger en arrière-plan]** . Les chemins de dossier sélectionnés doivent résider dans les dossiers que vous spécifiez dans le paramètre **[Dossiers à télécharger en arrière-plan]** . Spécifiez des chemins liés à la racine du profil local. Ne spécifiez pas de lecteur dans un nom de chemin d'accès.
Processus exclus	L'E/S des processus spécifiés est ignorée par View Persona Management. Vous pouvez avoir à ajouter certaines applications antivirus à la liste **[Processus exclus]** pour éviter tout problème de performance. Si une application antivirus ne dispose pas d'une fonction pour désactiver la récupération des fichiers hors ligne lors de ses analyses à la demande, le paramètre **[Processus exclus]** empêche l'application de récupérer les fichiers inutilement. Toutefois, View Persona Management ne réplique pas les modifications apportées aux fichiers et paramètres dans les profils des utilisateurs qui sont réalisés par des processus exclus. Pour ajouter des processus à la liste **[Processus exclus]** , activez ce paramètre, cliquez sur **[Afficher]** , tapez le nom du processus et cliquez sur **[OK]** . Par exemple : **`process.exe`**.

Paramètres de stratégie de groupe de redirection de dossiers

Avec des paramètres de stratégie de groupe de redirection de dossiers, vous pouvez rediriger des dossiers de profils d'utilisateur vers un partage de réseau. Lorsqu'un dossier est redirigé, toutes les données sont stockées directement sur le partage de réseau lors de la session utilisateur.

Vous pouvez utiliser ces paramètres pour rediriger des dossiers qui doivent être hautement disponibles. View Persona Management copie des mises à jour depuis le profil d'utilisateur local vers le profil distant au maximum une fois par minute, en fonction de la valeur que vous définissez pour l'intervalle de chargement du profil. Toutefois, si une panne réseau ou un échec sur le système local se produit, les mises à jour d'un utilisateur depuis la dernière réplication peuvent ne pas être enregistrées dans le profil distant. Dans les cas où les utilisateurs ne peuvent pas se permettre de perdre temporairement quelques minutes de leur travail récent, vous pouvez rediriger les dossiers qui stockent ces données critiques.

Les règles et recommandations suivantes s'appliquent à la redirection de dossiers :

- Lorsque vous activez ce paramètre pour un dossier, vous devez saisir le chemin d'accès UNC du partage de réseau vers lequel le dossier est redirigé.
- Si `%username%` ne fait pas partie du chemin de dossier que vous configurez, View Persona Management ajoute `%username%` au chemin d'accès UNC.
- Il vous est recommandé de configurer le chemin de dossier pour inclure `%username%`, mais assurez-vous que le dernier sous-dossier dans le chemin utilise le nom du dossier redirigé, tel que `My Videos`. Le dernier dossier dans le chemin est affiché sous la forme du nom de dossier sur le poste de travail de l'utilisateur. Pour plus d'informations, reportez-vous à la section « Configuration de chemins d'accès pour des dossiers redirigés », page 276.
- Vous configurez un paramètre séparé pour chaque dossier. Vous pouvez sélectionner des dossiers particuliers pour la redirection et en laisser d'autres sur le poste de travail View local. Vous pouvez également rediriger différents dossiers vers différents chemins d'accès UNC.
- Si un paramètre de redirection de dossiers est désactivé ou n'est pas configuré, le dossier est stocké sur le poste de travail View local et géré en fonction des paramètres de stratégie de groupe de View Persona Management.
- Si View Persona Management et des profils itinérants de Windows sont configurés pour rediriger le même dossier, la redirection de dossiers de View Persona Management est prioritaire sur les profils itinérants de Windows.
- La redirection de dossiers s'applique uniquement aux applications qui utilisent les API de shell Windows afin de rediriger des chemins de dossier communs. Par exemple, si une application écrit un fichier dans `%USERPROFILE%\AppData\Roaming`, le fichier est écrit dans le profil local et n'est pas redirigé vers l'emplacement réseau.

Vous pouvez spécifier des chemins de dossier qui sont exclus de la redirection de dossier. Reportez-vous à la section Tableau 9-3.

Avertissement View ne prend pas en charge l'activation de la redirection de dossier vers un dossier qui se trouve déjà dans un profil géré par View Persona Management. Cette configuration peut provoquer des échecs dans View Persona Management et entraîner la perte de données utilisateur.

Par exemple, si le dossier racine dans le référentiel de profils distant est `\\Server\%username%\`, et si vous redirigez des dossiers vers `\\Server\%username%\Desktop`, ces paramètres peuvent provoquer l'échec de la redirection de dossier dans View Persona Management et la perte du contenu qui se trouvait précédemment dans le dossier `\\Server\%username%\Desktop`.

Vous pouvez rediriger les dossiers suivants vers un partage de réseau :

- Données d'application (itinérantes)

- Contacts
- Cookies
- Poste de travail
- Téléchargements
- Favoris
- Historique
- Liens
- Mes documents
- Ma musique
- Mes images
- Mes vidéos
- Voisinage réseau
- Voisinage imprimante
- Éléments récents
- Jeux sauvegardés
- Recherches
- Menu Démarrer
- Éléments de démarrage
- Modèles
- Fichiers Internet temporaires

Certains dossiers sont disponibles uniquement dans les systèmes d'exploitation Windows Vista et supérieurs.

Tableau 9-3. Dossiers exclus de la redirection de dossier

Paramètre de stratégie de groupe	Description
Fichiers et dossiers exclus de la redirection de dossier	Les chemins de fichier et de dossier sélectionnés ne sont pas redirigés vers un partage de réseau. Dans certains scénarios, des fichiers et des dossiers spécifiques doivent rester dans le profil d'utilisateur local. Pour ajouter un chemin de dossier à la liste **[Fichiers et dossiers exclus de la redirection de dossier]** , activez ce paramètre, cliquez sur **[Afficher]** , tapez le nom du chemin et cliquez sur **[OK]** . Spécifiez des chemins de dossier liés à la racine du profil local de l'utilisateur. Par exemple : **`Poste de travail\Nouveau dossier`**.
Fichiers et dossiers exclus de la redirection de dossier (exceptions)	Les chemins de fichier et de dossier sélectionnés sont des exceptions aux chemins spécifiés dans le paramètre **[Fichiers et dossiers exclus de la redirection de dossier]** . Pour ajouter un chemin de dossier à la liste **[Fichiers et dossiers exclus de la redirection de dossier (exceptions)]** , activez ce paramètre, cliquez sur **[Afficher]** , tapez le nom du chemin et cliquez sur **[OK]** . Spécifiez les chemins de dossier qui résident dans un dossier spécifié dans le paramètre **[Dossiers exclus de la redirection de dossier]** et qui sont liés à la racine du profil local de l'utilisateur. Par exemple : **`Poste de travail\Nouveau dossier\Dossier unique`**.

Paramètres de stratégie de groupe d'interface utilisateur de poste de travail

Les paramètres de stratégie de groupe d'interface utilisateur de poste de travail contrôlent les paramètres de View Persona Management que les utilisateurs voient sur leurs postes de travail.

Paramètre de stratégie de groupe	Description
Hide local offline file icon (Masquer les icônes des fichiers hors ligne locaux)	Détermine si l'icône hors ligne est masquée lorsqu'un utilisateur voit les fichiers stockés localement qui appartiennent au profil d'utilisateur. L'activation de ce paramètre masque l'icône hors ligne dans Windows Explorer et dans la plupart des boîtes de dialogue de Windows. Par défaut, l'icône hors ligne est masquée.
Show progress when downloading large files (Afficher la progression lors du téléchargement de fichiers volumineux)	Détermine si une fenêtre de progression s'affiche sur le poste de travail d'un utilisateur quand le client récupère des fichiers volumineux depuis le référentiel distant. Quand ce paramètre est activé, vous pouvez spécifier la taille de fichier minimale, en mégaoctets, pour commencer à afficher la fenêtre de progression. La fenêtre s'affiche lorsque View Persona Management détermine que la quantité spécifiée de données sera récupérée depuis le référentiel distant. Cette valeur représente l'ensemble des fichiers récupérés en même temps. Par exemple, si la valeur du paramètre est 50 Mo et qu'un fichier de 40 Mo est récupéré, la fenêtre ne s'affiche pas. Si un fichier de 30 Mo est récupéré et que le premier fichier est toujours en cours de téléchargement, l'ensemble du téléchargement dépasse la valeur et la fenêtre de progression s'affiche. La fenêtre apparaît lorsque le téléchargement d'un fichier démarre. Par défaut, cette valeur est de 50 Mo. Par défaut, cette fenêtre de progression ne s'affiche pas.
Show critical errors to users via tray icon alerts (Afficher des erreurs critiques aux utilisateurs via des alertes d'icône de la barre d'état)	Affiche des alertes d'icône d'erreur critique dans la barre d'état du poste de travail lorsque des échecs de réplication ou de connectivité réseau se produisent. Par défaut, ces alertes d'icône sont masquées.

Paramètres de stratégie de groupe de journalisation

Les paramètres de stratégie de groupe de journalisation déterminent le nom, l'emplacement et le comportement des fichiers journaux de View Persona Management.

Paramètre de stratégie de groupe	Description
Nom de fichier de journalisation	Spécifie le nom de chemin complet du fichier journal de View Persona Management local. Sur des ordinateurs Windows 8 et Windows 7, le chemin d'accès par défaut est `ProgramData\VMware\VDM\logs\`*`filename`*. Sur des ordinateurs Windows XP, le chemin d'accès par défaut est *`All Users`*`\Application Data\VMware\VDM\logs\`*`filename`*. Le nom de fichier de journalisation par défaut est `VMWVvp.txt`.
Destination de journalisation	Détermine si tous les messages du journal sont écrits dans le fichier journal, dans le port de débogage ou dans les deux destinations. Par défaut, les messages de journalisation sont envoyés vers le fichier journal.

Paramètre de stratégie de groupe	Description
Indicateurs de journalisation	Détermine les types de messages à journaliser. Lorsque ce paramètre est configuré, vous pouvez sélectionner un ou tous les types de message de journalisation à générer : ■ messages d'erreur de journalisation ; ■ messages d'information de journalisation ; ■ messages de débogage de journalisation. Par défaut, des types de message de journalisation d'erreur et d'information sont générés.
Indicateurs de débogage	Détermine les types de messages de débogage à journaliser. View Persona Management traite les messages de débogage comme il traite les messages de journalisation. Lorsque ce paramètre est activé, vous pouvez sélectionner un ou tous les types de message de débogage à générer : ■ messages d'erreur de débogage ; ■ messages d'information de débogage ; ■ messages de port de débogage ; Par défaut, aucun message de débogage n'est généré.

Gestion de postes de travail de clone lié 10

Avec View Composer, vous pouvez mettre à jour des postes de travail de clone lié, réduire la taille de leurs données de système d'exploitation et rééquilibrer les machines virtuelles de clone lié sur des lecteurs de disque. Vous pouvez également gérer les disques persistants de View Composer associés à des clones liés.

- Réduire la taille du clone lié avec une actualisation de poste de travail page 289

  Une opération d'actualisation de poste de travail restaure le disque du système d'exploitation de chaque clone lié à son état et à sa taille d'origine, en réduisant les coûts de stockage.

- Mettre à jour des postes de travail de clone lié page 291

  Vous pouvez mettre à jour des postes de travail de clone lié en créant une nouvelle image de base sur la machine virtuelle parente et en utilisant la fonction de recomposition pour distribuer l'image mise à jour aux clones liés.

- Rééquilibrer des postes de travail de clone lié page 296

  Une opération de rééquilibrage de poste de travail redistribue de façon égale des postes de travail de clone lié sur des magasins de données disponibles.

- Gérer des disques persistants de View Composer page 300

  Vous pouvez détacher un disque persistant de View Composer d'un poste de travail de clone lié et l'attacher à un autre clone lié. Cette fonction vous permet de gérer des informations d'utilisateur séparément des postes de travail de clone lié.

Réduire la taille du clone lié avec une actualisation de poste de travail

Une opération d'actualisation de poste de travail restaure le disque du système d'exploitation de chaque clone lié à son état et à sa taille d'origine, en réduisant les coûts de stockage.

Si possible, planifiez les opérations d'actualisation au cours des heures creuses.

Pour voir des recommandations, reportez-vous à la section « Opérations d'actualisation de poste de travail », page 290.

Prérequis

- Décidez quand planifier une opération d'actualisation. Par défaut, View Composer démarre l'opération immédiatement.

  Vous pouvez planifier une seule opération d'actualisation à la fois pour un jeu donné de clones liés. Vous pouvez planifier plusieurs opérations d'actualisation si elles affectent différents clones liés.

- Décidez de forcer tous les utilisateurs à fermer leur session dès que l'opération commence ou d'attendre que chaque utilisateur ferme sa session avant d'actualiser le poste de travail de cet utilisateur.

Si vous forcez les utilisateurs à fermer leurs sessions, View Manager informe les utilisateurs avant qu'ils soient déconnectés et les autorise à fermer leurs applications et leur session.

Si vous forcez les utilisateurs à fermer leur session, le nombre maximal d'opérations d'actualisation simultanées sur les postes de travail dont les sessions doivent être fermées est égal à la moitié de la valeur du paramètre **[Max concurrent View Composer maintenance operations (Nombre maximal d'opérations simultanées de maintenance View Composer)]** . Par exemple, si ce paramètre a la valeur 24 et que vous forciez les utilisateurs à fermer leur session, le nombre maximal d'opérations d'actualisation simultanées sur les postes de travail dont les sessions doivent être fermées est égal à 12.

- Si votre déploiement comporte des instances répliquées de Serveur de connexion View, vérifiez que toutes les instances ont la même version.

Procédure

1 Dans View Administrator, cliquez sur **[Inventory (Inventaire)] > [Pools]** .

2 Sélectionnez le pool à actualiser en double-cliquant sur l'ID de pool dans la colonne de gauche.

3 Choisissez d'actualiser tout le pool ou des postes de travail sélectionnés.

Option	Action
To refresh all desktops in the pool (Actualiser tous les postes de travail du pool)	Sur la page du pool sélectionné, cliquez sur l'onglet **[Settings (Paramètres)]** .
To refresh selected desktops (Actualiser des postes de travail sélectionnés)	a Sur la page du pool sélectionné, cliquez sur l'onglet **[Inventory (Inventaire)]** . b Sélectionnez les postes de travail à actualiser.

4 Cliquez sur **[View Composer] > [Actualiser]** .

5 Suivez les instructions de l'assistant pour actualiser les postes de travail de clone lié.

Les disques du système d'exploitation sont réduits à leur taille d'origine.

Dans vCenter Server, vous pouvez surveiller la progression de l'opération d'actualisation sur les machines virtuelles de clone lié.

Dans View Administrator, vous pouvez surveiller l'opération en cliquant sur **[Inventory (Inventaire)] > [Pools]** , en sélectionnant l'ID de pool et en cliquant sur l'onglet **[Tasks (Tâches)]** . Vous pouvez cliquer sur **[Cancel Task (Annuler la tâche)]** , **[Pause Task (Suspendre la tâche)]** ou **[Resume Task (Reprendre la tâche)]** pour terminer une tâche, suspendre une tâche ou reprendre une tâche suspendue.

Opérations d'actualisation de poste de travail

À mesure que les utilisateurs interagissent avec des postes de travail de clone lié, les disques du système d'exploitation des clones croissent. Une opération d'actualisation du poste de travail restaure les disques du système d'exploitation à leur état et à leur taille d'origine, en réduisant les coûts de stockage.

Une opération d'actualisation n'affecte pas les disques persistants de View Composer.

Un clone lié utilise moins d'espace de stockage que la machine virtuelle parente, qui contient toutes les données de système d'exploitation. Toutefois, le disque du système d'exploitation d'un clone croît chaque fois que des données y sont inscrites à partir du système d'exploitation client.

Lorsque View Composer crée un clone lié, il prend un snapshot du disque du système d'exploitation du clone. Le snapshot identifie de façon unique la machine virtuelle de clone lié. Une opération d'actualisation rétablit le disque du système d'exploitation vers le snapshot.

View Composer peut actualiser un clone lié en deux fois moins de temps nécessaire pour supprimer et recréer le clone.

Appliquez ces recommandations aux opérations d'actualisation :

- Vous pouvez actualiser un pool de postes de travail à la demande, sous forme d'événement planifié, ou quand les données de système d'exploitation atteignent une taille spécifiée.

  Vous pouvez planifier une seule opération d'actualisation à la fois pour un jeu donné de clones liés. Si vous démarrez une opération d'actualisation immédiatement, elle remplace toutes les tâches planifiées précédemment.

  Vous pouvez planifier plusieurs opérations d'actualisation si elles affectent différents clones liés.

  Avant de planifier une nouvelle opération d'actualisation, vous devez annuler toutes les tâches planifiées précédemment.

- Vous pouvez actualiser des pools d'affectation dédiée et d'affectation flottante.
- Vous ne pouvez pas actualiser des postes de travail exécutant des sessions locales.
- Une actualisation ne peut avoir lieu que lorsque les utilisateurs sont déconnectés de leurs postes de travail View.
- Une actualisation conserve les informations uniques sur l'ordinateur définies par QuickPrep ou Sysprep. Vous n'avez pas à réexécuter Sysprep après une actualisation pour restaurer le SID ou les GUID de logiciels tiers installés sur le lecteur système.
- Lorsque vous avez recomposé un clone lié, View Manager prend un nouveau snapshot du disque du système d'exploitation du clone lié. Les opérations d'actualisation futures restaurent les données de système d'exploitation sur ce snapshot, pas sur celui pris à l'origine lors de la première création du clone lié.

  Si vous utilisez la technologie de snapshot NFS native (VAAI) pour générer des clones liés, les périphériques NAS de certains fournisseurs prennent des snapshots du disque de réplica lorsqu'ils actualisent les disques du système d'exploitation des clones liés. Ces périphériques NAS ne prennent pas en charge la prise de snapshots directs du disque du système d'exploitation de chaque clone.

- Vous pouvez définir un nombre minimum de postes de travail approvisionnés prêts auxquels les utilisateurs peuvent se connecter lors de l'opération d'actualisation. Reportez-vous à la section « Maintien des postes de travail de clone lié approvisionnés et prêts lors d'opérations de View Composer », page 133.

Remarque Vous pouvez ralentir la croissance de clone liés en redirigeant leurs fichiers d'échange et leurs fichiers temporaires de système vers un disque temporaire. Lorsqu'un clone lié est mis hors tension, View Manager remplace le disque temporaire par une copie du disque temporaire d'origine que View Composer a créé avec le pool de clone lié. Cette opération réduit le disque temporaire à sa taille d'origine.

Vous pouvez configurer cette option lorsque vous créez un pool de clone lié.

Mettre à jour des postes de travail de clone lié

Vous pouvez mettre à jour des postes de travail de clone lié en créant une nouvelle image de base sur la machine virtuelle parente et en utilisant la fonction de recomposition pour distribuer l'image mise à jour aux clones liés.

- Préparer une machine virtuelle parente pour recomposer des postes de travail de clone lié page 292

  Avant de recomposer un pool de postes de travail de clone lié, vous devez mettre à jour la machine virtuelle parente que vous avez utilisé comme image de base pour les clones liés.

- Recomposer des postes de travail de clone lié page 292

  La recomposition de poste de travail met à jour simultanément tous les postes de travail de clone lié ancrés à une machine virtuelle parente.

- Recomposer des postes de travail de clone lié pouvant s'exécuter en mode local page 294

  Vous pouvez recomposer des postes de travail de clone lié pouvant s'exécuter en mode local. Toutefois, les postes de travail doivent être restitués ou restaurés sur le datacenter avant que l'opération de recomposition puisse avoir lieu.

- Mise à jour de clones liés avec la recomposition de poste de travail page 295

  Dans une recomposition de poste de travail, vous pouvez fournir des correctifs de système d'exploitation, installer ou mettre à jour des applications, ou modifier les réglages matériels du poste de travail dans tous les clones liés d'un pool de postes de travail.

- Corriger une recomposition échouée page 296

  Vous pouvez corriger une recomposition qui a échoué. Vous pouvez également agir si vous recomposez accidentellement des clones liés en utilisant une image de base différente de celle que vous vouliez utiliser.

Préparer une machine virtuelle parente pour recomposer des postes de travail de clone lié

Avant de recomposer un pool de postes de travail de clone lié, vous devez mettre à jour la machine virtuelle parente que vous avez utilisé comme image de base pour les clones liés.

View Composer ne prend pas en charge la recomposition de clones liés qui utilisent un système d'exploitation sur une machine virtuelle parente qui utilise un système d'exploitation différent. Par exemple, vous ne pouvez pas utiliser un snapshot d'une machine virtuelle parente Windows 8, Windows 7 ou Windows Vista pour recomposer un clone lié de Windows XP.

Procédure

1 Dans vCenter Server, mettez à jour la machine virtuelle parente pour la recomposition.

   - Installez des correctifs de système d'exploitation ou des packs de service, de nouvelles applications, des mises à jour d'application ou faites d'autres modifications dans la machine virtuelle parente.
   - Vous pouvez également préparer une autre machine virtuelle à être sélectionnée comme nouveau parent lors de la recomposition.

2 Dans vCenter Server, mettez hors tension la machine virtuelle parente mise à jour ou la nouvelle machine virtuelle parente.

3 Dans vCenter Server, prenez un snapshot de la machine virtuelle parente.

Suivant

Recomposez le pool de postes de travail de clone lié.

Recomposer des postes de travail de clone lié

La recomposition de poste de travail met à jour simultanément tous les postes de travail de clone lié ancrés à une machine virtuelle parente.

Si possible, planifiez les recompositions au cours des heures creuses.

Prérequis

- Vérifiez que vous avez un snapshot de la machine virtuelle parente. Reportez-vous à la section « Préparer une machine virtuelle parente pour recomposer des postes de travail de clone lié », page 292.
- Familiarisez-vous avec les recommandations sur la recomposition. Reportez-vous à la section « Mise à jour de clones liés avec la recomposition de poste de travail », page 295.

- Décidez quand planifier la recomposition. Par défaut, View Composer démarre la recomposition immédiatement.

  Vous ne pouvez planifier qu'une seule recomposition à la fois pour un jeu donné de clones liés. Vous pouvez planifier plusieurs recompositions si elles affectent différents clones liés.

- Décidez de forcer tous les utilisateurs à fermer leur session dès que la recomposition commence ou d'attendre que chaque utilisateur ferme sa session avant de recomposer le poste de travail de cet utilisateur.

  Si vous forcez les utilisateurs à fermer leurs sessions, View Manager informe les utilisateurs avant qu'ils soient déconnectés et les autorise à fermer leurs applications et leur session.

  Si vous forcez les utilisateurs à fermer leur session, le nombre maximal d'opérations de recomposition simultanées sur les postes de travail dont les sessions doivent être fermées est égal à la moitié de la valeur du paramètre **[Max concurrent View Composer maintenance operations (Nombre maximal d'opérations simultanées de maintenance View Composer)]** . Par exemple, si ce paramètre a la valeur 24 et que vous forciez les utilisateurs à fermer leur session, le nombre maximal d'opérations de recomposition simultanées sur les postes de travail dont les sessions doivent être fermées est égal à 12.

- Décidez d'arrêter l'approvisionnement à la première erreur. Si vous sélectionnez cette option et si une erreur se produit lorsque View Composer approvisionne un clone lié, l'approvisionnement s'arrête pour tous les clones dans le pool. Vous pouvez sélectionner cette option pour vous assurer que des ressources telles que le stockage ne sont pas consommées inutilement.

  La sélection de l'option **[Stop at first error (Arrêter à la première erreur)]** n'affecte pas la personnalisation. Si une erreur de personnalisation se produit sur un clone lié, l'approvisionnement et la personnalisation des autres clones continuent.

- Vérifiez que l'approvisionnement du pool est activé. Dans le cas contraire, View Manager empêche la personnalisation des postes de travail après recomposition.

- Si votre déploiement comporte des instances répliquées de Serveur de connexion View, vérifiez que toutes les instances ont la même version.

Procédure

1 Dans View Administrator, cliquez sur **[Inventory (Inventaire)] > [Pools]** .

2 Sélectionnez le pool à recomposer en double-cliquant sur l'ID de pool dans la colonne de gauche.

3 Choisissez de recomposer tout le pool ou des postes de travail sélectionnés.

Option	Action
To recompose all desktops in the pool (Recomposer tous les postes de travail du pool)	Sur la page du pool sélectionné, cliquez sur l'onglet **[Settings (Paramètres)]** .
To recompose selected desktops (Recomposer des postes de travail sélectionnés)	a Sur la page du pool sélectionné, cliquez sur l'onglet **[Inventory (Inventaire)]** . b Sélectionnez les postes de travail à recomposer.

4 Cliquez sur **[View Composer] > [Recomposer]** .

5 Suivez les instructions de l'assistant pour recomposer les postes de travail de clone lié.

  Si vous recomposez tout le pool dans l'onglet **[Settings (Paramètres)]** , vous pouvez cocher la case **[Change the default image for new desktops (Modifier l'image par défaut pour les nouveaux postes de travail)]** . Avec ce paramètre, les nouveaux postes de travail créés dans le pool utilisent l'image de base mise à jour. Ce paramètre est coché par défaut.

  Sur la page Ready to Complete, vous pouvez cliquer sur **[Show Details]** pour afficher les postes de travail de clone lié qui seront recomposés.

Les postes de travail de clone lié sont actualisés et mis à jour. Les disques du système d'exploitation sont réduits à leur taille d'origine.

Dans un pool d'affectation dédiée, les clones liés non affectés sont supprimés et recréés. Le nombre spécifié de postes de travail de rechange est conservé.

Dans un pool d'affectation flottante, tous les clones liés sélectionnés sont recomposés.

Dans vCenter Server, vous pouvez surveiller la progression de la recomposition sur les machines virtuelles de clone lié.

Dans View Administrator, vous pouvez surveiller l'opération en cliquant sur **[Inventory (Inventaire)] > [Pools]** , en sélectionnant l'ID de pool et en cliquant sur l'onglet **[Tasks (Tâches)]** . Vous pouvez cliquer sur **[Cancel Task (Annuler la tâche)]** , **[Pause Task (Suspendre la tâche)]** ou **[Resume Task (Reprendre la tâche)]** pour terminer une tâche, suspendre une tâche ou reprendre une tâche suspendue.

Remarque Si vous avez utilisé une spécification de personnalisation Sysprep pour personnaliser les clones liés lorsque vous avez créé le pool de postes de travail, de nouveaux SID peuvent être générés pour les machines virtuelles recomposées. Pour plus d'informations, reportez-vous à la section « Recomposition de clones liés personnalisés avec Sysprep », page 120.

Recomposer des postes de travail de clone lié pouvant s'exécuter en mode local

Vous pouvez recomposer des postes de travail de clone lié pouvant s'exécuter en mode local. Toutefois, les postes de travail doivent être restitués ou restaurés sur le datacenter avant que l'opération de recomposition puisse avoir lieu.

Prérequis

- Familiarisez-vous avec les recommandations sur la recomposition. Reportez-vous à la section « Mise à jour de clones liés avec la recomposition de poste de travail », page 295.
- Familiarisez-vous avec la procédure de mise à jour de l'image de base et de recomposition des postes de travail de clone lié. Reportez-vous à la section « Préparer une machine virtuelle parente pour recomposer des postes de travail de clone lié », page 292 et « Recomposer des postes de travail de clone lié », page 292.
- Familiarisez-vous avec la procédure de publication d'images de base dans le référentiel de Transfer Server. Reportez-vous à la section « Publier des fichiers de package dans le référentiel de Serveur de transfert », page 364.

Procédure

1 Restituez ou restaurez les postes de travail de clone lié locaux créés à partir de l'image de base.

2 Initiez l'opération de recomposition.

L'opération de recomposition ignore les postes de travail en mode local.

3 Publiez une image de base recomposée pour le référentiel de Transfer Server.

Les postes de travail de clone lié sont mis à jour avec la nouvelle image de base.

La prochaine fois que les utilisateurs empruntent leurs postes de travail de clone lié, View Transfer Server télécharge l'image de base mise à jour à partir du référentiel de Transfer Server vers les ordinateurs client. View Transfer Server télécharge également les disques du système d'exploitation des clones liés et les disques persistants de View Composer sur les ordinateurs client.

Remarque Les postes de travail qui se trouvaient en mode local lors de l'opération de recomposition utilisent toujours l'ancienne image de base. Ces postes de travail ne sont pas recomposés lorsque des utilisateurs les restituent.

Mise à jour de clones liés avec la recomposition de poste de travail

Dans une recomposition de poste de travail, vous pouvez fournir des correctifs de système d'exploitation, installer ou mettre à jour des applications, ou modifier les réglages matériels du poste de travail dans tous les clones liés d'un pool de postes de travail.

Pour recomposer des postes de travail de clone lié, vous mettez à jour la machine virtuelle parente dans vCenter Server ou vous sélectionnez une machine virtuelle différente pour devenir le nouveau parent. Ensuite, vous prenez un snapshot de la nouvelle configuration de machine virtuelle parente.

Vous pouvez modifier la machine virtuelle parente sans affecter les clones liés car ils sont liés au réplica, pas directement au parent.

Ensuite, vous initiez la recomposition, en sélectionnant le snapshot à utiliser comme nouvelle image de base pour le pool de postes de travail. View Composer crée un nouveau réplica, copie le disque du système d'exploitation reconfiguré sur les clones liés et ancre les clones liés au nouveau réplica.

La recomposition actualise également les clones liés, en réduisant la taille de leurs disques du système d'exploitation.

Les recompositions de poste de travail n'affectent pas les disques persistants de View Composer.

Appliquez ces recommandations aux recompositions :

- Vous pouvez recomposer des pools d'affectation dédiée et d'affectation flottante.
- Vous pouvez recomposer un pool de postes de travail à la demande ou sous forme d'événement planifié.

  Vous ne pouvez planifier qu'une seule recomposition à la fois pour un jeu donné de clones liés. Avant de planifier une nouvelle recomposition, vous devez annuler toutes les tâches planifiées précédemment ou attendre la fin de l'opération précédente. Avant de démarrer une nouvelle recomposition sans attendre, vous devez annuler toutes les tâches planifiées précédemment.

  Vous pouvez planifier plusieurs recompositions si elles affectent différents clones liés.
- Vous pouvez recomposer des clones liés sélectionnés ou tous les clones liés d'un pool de postes de travail.
- Lorsque des clones liés différents dans un pool sont dérivés de différents snapshots de l'image de base ou d'images de base différentes, le pool comporte plusieurs réplicas.
- Vous ne pouvez pas recomposer des postes de travail exécutés en mode local. Les postes de travail locaux doivent être restitués ou restaurés sur le datacenter avant qu'une opération de recomposition puisse avoir lieu.
- Une recomposition ne peut avoir lieu que lorsque les utilisateurs ferment leur session sur leurs postes de travail View.
- Vous ne pouvez pas recomposer des clones liés qui utilisent un système d'exploitation vers une nouvelle machine virtuelle parente ou une machine virtuelle parente mise à jour qui utilise un système d'exploitation différent.
- Vous ne pouvez pas recomposer de clones liés sur un matériel avec une version inférieure à la version actuelle. Par exemple, vous ne pouvez pas recomposer des clones avec le matériel version 8 sur une machine virtuelle parente avec le matériel version 7.

- Vous pouvez définir un nombre minimal de postes de travail approvisionnés prêts auxquels les utilisateurs peuvent se connecter lors de l'opération de recomposition. Reportez-vous à la section « Maintien des postes de travail de clone lié approvisionnés et prêts lors d'opérations de View Composer », page 133.

Remarque Si vous avez utilisé une spécification de personnalisation Sysprep pour personnaliser les clones liés lorsque vous avez créé le pool de postes de travail, de nouveaux SID peuvent être générés pour les machines virtuelles recomposées. Pour plus d'informations, reportez-vous à la section « Recomposition de clones liés personnalisés avec Sysprep », page 120.

Corriger une recomposition échouée

Vous pouvez corriger une recomposition qui a échoué. Vous pouvez également agir si vous recomposez accidentellement des clones liés en utilisant une image de base différente de celle que vous vouliez utiliser.

Problème

Les postes de travail sont dans un état erroné ou périmé à la suite d'une recomposition échouée.

Cause

Une panne du système ou un problème s'est peut-être produit sur l'hôte de vCenter Server, dans vCenter Server ou sur un magasin de données lors de la recomposition.

La recomposition peut également avoir utilisé un snapshot de machine virtuelle avec un système d'exploitation différent du système d'exploitation de la machine virtuelle parente d'origine. Par exemple, vous pouvez avoir utilisé un snapshot de Windows 7 ou supérieur pour recomposer des clones liés de Windows XP.

Solution

1 Sélectionnez le snapshot utilisé dans la dernière recomposition réussie.

Vous pouvez également sélectionner un nouveau snapshot pour mettre à jour les clones liés vers un nouvel état.

Le snapshot doit utiliser le même système d'exploitation que le snapshot de la machine virtuelle parente d'origine.

2 Recomposez de nouveau le pool.

View Composer crée une image de base depuis le snapshot et recrée les disques du système d'exploitation de clone lié.

Les disques persistants de View Composer qui contiennent des données et des paramètres d'utilisateur sont conservés lors de la recomposition.

En fonction des conditions de la recomposition incorrecte, vous devrez peut-être actualiser ou rééquilibrer les clones liés à la place ou en plus de les recomposer.

Remarque Si vous ne configurez pas les disques persistants de View Composer, toutes les recompositions suppriment les modifications générées par l'utilisateur dans les postes de travail de clone lié.

Rééquilibrer des postes de travail de clone lié

Une opération de rééquilibrage de poste de travail redistribue de façon égale des postes de travail de clone lié sur des magasins de données disponibles.

Vous pouvez également utiliser le réquilibrage pour migrer des postes de travail de clone vers un autre magasin de données. N'utilisez pas vSphere Client ni vCenter Server pour migrer ou gérer les machines virtuelles de clone lié. Reportez-vous à la section « Migrer les postes de travail de clone lié vers un autre magasin de données », page 299.

Si possible, planifiez les opérations de rééquilibrage au cours des heures creuses.

Pour voir des recommandations, reportez-vous à la section « Rééquilibrage de clones liés sur des lecteurs logiques », page 298.

Prérequis

- Familiarisez-vous avec l'opération de rééquilibrage. Reportez-vous à la section « Rééquilibrage de clones liés sur des lecteurs logiques », page 298.
- Décidez quand planifier une opération de rééquilibrage. Par défaut, View Composer démarre l'opération immédiatement.

  Vous pouvez planifier une seule opération de rééquilibrage à la fois pour un jeu donné de clones liés. Vous pouvez planifier plusieurs opérations de rééquilibrage si elles affectent différents clones liés.
- Décidez de forcer tous les utilisateurs à fermer leur session dès que l'opération commence ou d'attendre que chaque utilisateur ferme sa session avant de rééquilibrer le poste de travail de cet utilisateur.

  Si vous forcez les utilisateurs à fermer leurs sessions, View Manager informe les utilisateurs avant qu'ils soient déconnectés et les autorise à fermer leurs applications et leur session.

  Si vous forcez les utilisateurs à fermer leur session, le nombre maximal d'opérations de réquilibrage simultanées sur les postes de travail dont les sessions doivent être fermées est égal à la moitié de la valeur du paramètre **[Max concurrent View Composer maintenance operations (Nombre maximal d'opérations simultanées de maintenance View Composer)]** . Par exemple, si ce paramètre a la valeur 24 et que vous forcez les utilisateurs à fermer leur session, le nombre maximal d'opérations de rééquilibrage simultanées sur les postes de travail dont les sessions doivent être fermées est égal à 12.
- Vérifiez que l'approvisionnement du pool est activé. Dans le cas contraire, View Manager empêche la personnalisation des postes de travail après rééquilibrage.
- Si votre déploiement comporte des instances répliquées de Serveur de connexion View, vérifiez que toutes les instances ont la même version.

Procédure

1 Dans View Administrator, cliquez sur **[Inventory (Inventaire)] > [Pools]** .

2 Sélectionnez le pool à rééquilibrer en double-cliquant sur l'ID de pool dans la colonne de gauche.

3 Choisissez de rééquilibrer tout le pool ou des postes de travail sélectionnés.

Option	Action
To rebalance all desktops in the pool (Rééquilibrer tous les postes de travail du pool)	Sur la page du pool sélectionné, cliquez sur l'onglet **[Settings (Paramètres)]** .
To rebalance selected desktops (Rééquilibrer des postes de travail sélectionnés)	a Sur la page du pool sélectionné, cliquez sur l'onglet **[Inventory (Inventaire)]** . b Sélectionnez les postes de travail à rééquilibrer.

4 Cliquez sur **[View Composer] > [Rebalance (Rééquilibrer)]** .

5 Suivez les instructions de l'assistant pour rééquilibrer les postes de travail de clone lié.

Les postes de travail de clone lié sont actualisés et rééquilibrés. Les disques du système d'exploitation sont réduits à leur taille d'origine.

Dans View Administrator, vous pouvez surveiller l'opération en cliquant sur **[Inventory (Inventaire)] > [Pools]** , en sélectionnant l'ID de pool et en cliquant sur l'onglet **[Tasks (Tâches)]** . Vous pouvez cliquer sur **[Cancel Task (Annuler la tâche)]** , **[Pause Task (Suspendre la tâche)]** ou **[Resume Task (Reprendre la tâche)]** pour terminer une tâche, suspendre une tâche ou reprendre une tâche suspendue.

Rééquilibrage de clones liés sur des lecteurs logiques

Une opération de rééquilibrage de poste de travail redistribue de façon égale des postes de travail de clone lié sur des lecteurs logiques disponibles. Cela économise de l'espace de stockage sur des lecteurs surchargés et garantit qu'aucun lecteur n'est sous-utilisé.

Lorsque vous créez des pools de postes de travail de clone lié volumineux et que vous utilisez plusieurs LUN (Logical Unit Number), il est possible que l'espace ne soit pas utilisé efficacement si le dimensionnement initial n'était pas précis. Si vous définissez un niveau de surcharge de stockage élevé, les clones liés peuvent croître rapidement et consommer tout l'espace libre sur le magasin de données.

Lorsque les machines virtuelles utilisent 95 % de l'espace sur le magasin de données, View Manager génère une entrée de journal d'avertissement.

Le rééquilibrage actualise également les clones liés, en réduisant la taille de leurs disques du système d'exploitation. Il n'affecte pas les disques persistants de View Composer.

Appliquez ces recommandations aux rééquilibrages de postes de travail :

- Vous pouvez rééquilibrer des pools d'affectation dédiée et d'affectation flottante.
- Vous pouvez rééquilibrer des clones liés sélectionnés ou tous les clones dans un pool.
- Vous pouvez rééquilibrer un pool de postes de travail à la demande ou sous forme d'événement planifié.

  Vous pouvez planifier une seule opération de rééquilibrage à la fois pour un jeu donné de clones liés. Si vous démarrez une opération de rééquilibrage immédiatement, elle remplace toutes les tâches planifiées précédemment.

  Vous pouvez planifier plusieurs opérations de rééquilibrage si elles affectent différents clones liés.

  Avant de planifier une nouvelle opération de rééquilibrage, vous devez annuler toutes les tâches planifiées précédemment.
- Vous ne pouvez rééquilibrer que des postes de travail se trouvant en état Disponible, Erreur ou Personnalisation sans annulation prévue ou en attente.
- Il est conseillé de ne pas mélanger les machines virtuelles de clone lié avec d'autres types de machines virtuelles sur le même magasin de données. De cette façon, View Composer peut rééquilibrer toutes les machines virtuelles sur le magasin de données.
- Si vous modifiez un pool, ainsi que l'hôte ou le cluster et les magasins de données sur lesquels des clones liés sont stockés, vous pouvez uniquement rééquilibrer les clones liés si l'hôte ou le cluster sélectionné a un accès complet aux magasins de données initiaux et nouveaux. Tous les hôtes du nouveau cluster doivent avoir accès aux magasins de données initiaux et nouveaux.

  Par exemple, vous pouvez créer un pool de clone lié sur un hôte autonome et sélectionner un magasin de données local pour stocker les clones. Si vous modifiez le pool et sélectionnez un cluster et un magasin de données partagé, toute opération de rééquilibrage échouera car les hôtes du cluster ne peuvent pas accéder au magasin de données local d'origine.
- Vous pouvez définir un nombre minimal de postes de travail approvisionnés prêts auxquels les utilisateurs peuvent se connecter lors de l'opération de rééquilibrage. Reportez-vous à la section « Maintien des postes de travail de clone lié approvisionnés et prêts lors d'opérations de View Composer », page 133.

Migrer les postes de travail de clone lié vers un autre magasin de données

Pour migrer les machines virtuelles de clone lié d'un groupe de magasin de données vers un autre, utilisez le rééquilibrage.

Lorsque vous utilisez le rééquilibrage, View Composer gère le mouvement des clones liés entre les magasins de données. View Composer maintient l'accès au réplica des clones liés pendant et après le rééquilibrage. Si nécessaire, View Composer crée une instance du réplica dans le magasin de données de destination.

Remarque N'utilisez pas vSphere Client ni vCenter Server pour migrer ou gérer les machines virtuelles de clone lié. N'utilisez pas Storage vMotion pour migrer des machines virtuelles de clone lié vers d'autres magasins de données.

Prérequis

Familiarisez-vous avec l'opération de rééquilibrage. Reportez-vous aux sections « Rééquilibrer des postes de travail de clone lié », page 296 et« Rééquilibrage de clones liés sur des lecteurs logiques », page 298.

Procédure

1 Dans View Administrator, sélectionnez le pool de clones liés à migrer et cliquez sur **[Edit (Modifier)]** .

2 Dans l'onglet des paramètres vCenter, accédez à **[Datastores (Magasins de données)]** et cliquez sur **[Browse (Parcourir)]** .

3 Dans la page Select Linked Clone Datastores (Sélectionner des magasins de données de clone lié), désélectionnez les magasins de données qui contiennent les clones liés, sélectionnez les magasins de données de destination et cliquez sur **[OK]** .

4 Dans la fenêtre de modification de *pool name*, cliquez sur **[OK]** .

5 Dans la page *pool name*, cliquez sur **[View Composer]** > **[Rebalance (Rééquilibrer)]** .

6 Suivez les instructions de l'assistant pour rééquilibrer les postes de travail de clone lié.

Les postes de travail de clone lié sont actualisés et migrés vers les magasins de données de destination.

Noms de fichier de disques de clone lié après une opération de rééquilibrage

Lorsque vous rééquilibrez des postes de travail de clone lié, vCenter Server modifie les noms de fichier de disques persistants de View Composer et de disques de données supprimables dans des clones liés déplacés vers un nouveau magasin de données.

Le noms de fichier d'origine identifient le type de disque. Les disques renommés n'incluent pas les étiquettes d'identification.

Un disque persistant d'origine a un nom de fichier avec une étiquette `user-disk` : *`desktop_name`*`-vdm-user-disk-D-`*`ID`*`.vmdk`.

Un disque de données supprimables d'origine a un nom de fichier avec une étiquette `disposable` : *`desktop_name`*`-vdm-disposable-`*`ID`*`.vmdk`.

Quand une opération de rééquilibrage déplace un clone lié vers un nouveau magasin de données, vCenter Server utilise une syntaxe de nom de fichier commun pour les deux types de disques : *`desktop_name_n`*`.vmdk`.

Gérer des disques persistants de View Composer

Vous pouvez détacher un disque persistant de View Composer d'un poste de travail de clone lié et l'attacher à un autre clone lié. Cette fonction vous permet de gérer des informations d'utilisateur séparément des postes de travail de clone lié.

Disques persistants de View Composer

Avec View Composer, vous pouvez configurer des données de système d'exploitation et des informations utilisateur sur des disques séparés dans des postes de travail de clone lié. View Composer conserve les informations utilisateur sur le disque persistant lorsque les données de système d'exploitation sont mises à jour, actualisées ou rééquilibrées.

Un disque persistant de View Composer contient des paramètres d'utilisateur et d'autres données générées par l'utilisateur. Vous créez des disques persistants lorsque vous créez un pool de postes de travail de clone lié. Reportez-vous à la section « Feuille de calcul pour créer un pool de postes de travail de clone lié », page 103.

Vous pouvez détacher un disque persistant de son poste de travail de clone lié et stocker le disque sur son magasin de données d'origine ou un autre magasin de données. Après avoir détaché le disque, la machine virtuelle de clone lié est supprimée. Un disque persistant détaché n'est plus associé à aucun poste de travail.

Vous pouvez utiliser plusieurs méthodes pour attacher un disque persistant détaché à un autre poste de travail de clone lié. Cette flexibilité a plusieurs utilisations :

- Lorsqu'un clone lié est supprimé, vous pouvez conserver les données utilisateur.
- Lorsqu'un employé quitte l'entreprise, un autre employé peut accéder aux données utilisateur de l'employé sur le départ.
- Un utilisateur avec plusieurs postes de travail peut consolider les données utilisateur sur un seul poste de travail.
- Si une machine virtuelle devient inaccessible dans vCenter Server, mais que le disque persistant est intact, vous pouvez importer le disque persistant et créer un nouveau clone lié en utilisant le disque.

Remarque Vous ne pouvez pas détacher un disque persistant d'un clone lié Windows XP et recréer ou attacher le disque persistant à un clone lié Windows 8, Windows 7 ou Windows Vista. Les disques persistants doivent être reconnectés au système d'exploitation qui avait été utilisé lors de leur création.

View Manager peut gérer les disques persistants à partir de pools de clone lié créés dans View Manager 4.5 ou supérieur. Les disques persistants créés dans les versions précédentes de View Manager ne peuvent pas être gérés et n'apparaissent pas sur la page Disques persistants de View Administrator.

Détacher un disque persistant de View Composer

Lorsque vous détachez un disque persistant de View Composer d'un poste de travail de clone lié, le disque est stocké et le clone lié est supprimé. En détachant un disque persistant, vous pouvez stocker et réutiliser des informations spécifiques de l'utilisateur avec un autre poste de travail.

Procédure

1 Dans View Administrator, cliquez sur **[Inventaire] > [Disques persistants]** .

2 Sélectionnez le disque persistant à détacher.

3 Cliquez sur **[Détacher]** .

4 Choisissez l'emplacement de stockage du disque persistant.

Option	Description
Utiliser le magasin de données actuel	Stockez le disque persistant sur le magasin de données où il se situe actuellement.
Utiliser le magasin de données suivant	Sélectionnez un nouveau magasin de données sur lequel stocker le disque persistant. Cliquez sur **[Parcourir]** , cliquez sur la flèche vers le bas et sélectionnez un nouveau magasin de données dans le menu **[Choisir un magasin de données]** . Vous ne pouvez pas sélectionner un magasin de données local pour stocker un disque persistant détaché. Vous devez utiliser un magasin de données partagé.

Le disque persistant de View Composer est enregistré sur le magasin de données. Le poste de travail de clone lié est supprimé et n'apparaît pas dans View Administrator.

Attacher un disque persistant de View Composer à un autre poste de travail de clone lié

Vous pouvez attacher un disque persistant détaché à un autre poste de travail de clone lié. Le fait d'attacher un disque persistant rend les paramètres et les informations d'utilisateur du disque disponibles à l'utilisateur de l'autre poste de travail.

Vous attachez un disque persistant détaché comme disque secondaire sur le poste de travail de clone lié sélectionné. L'utilisateur du nouveau poste de travail a accès au disque secondaire et aux informations et paramètres d'utilisateur existants sur le poste de travail.

Prérequis

Vérifiez que le poste de travail sélectionné utilise le même système d'exploitation que celui du clone lié dans lequel le disque persistant a été créé.

Procédure

1 Dans View Administrator, cliquez sur **[Inventory (Inventaire)] > [Disques persistants]** .

2 Cliquez sur l'onglet **[Detached (Détaché)]** .

3 Sélectionnez le disque persistant.

4 Cliquez sur **[Attach (Attacher)]** .

5 Sélectionnez un poste de travail de clone lié auquel attacher le disque persistant.

6 Sélectionnez **[Attach as a secondary disk (Attacher comme disque secondaire)]** .

7 Cliquez sur **[Finish (Terminer)]** .

Suivant

Assurez-vous que l'utilisateur du poste de travail de clone lié possède des privilèges suffisants pour utiliser le disque secondaire attaché. Par exemple, si l'utilisateur d'origine possède certaines autorisations d'accès sur le disque persistant, et que le disque persistant est attaché en tant que lecteur `D` sur le nouveau poste de travail, le nouvel utilisateur du poste de travail doit posséder les autorisations d'accès de l'utilisateur d'origine sur le lecteur `D`.

Ouvrez une session sur le système d'exploitation client du poste de travail en tant qu'administrateur et affectez des privilèges appropriés au nouvel utilisateur du poste de travail.

Modifier le pool ou l'utilisateur d'un disque persistant de View Composer

Vous pouvez affecter un disque persistant détaché de View Composer à un nouveau pool ou à un nouvel utilisateur si le pool ou l'utilisateur d'origine a été supprimé de View Manager.

Un disque persistant détaché est toujours associé à son pool ou à son utilisateur d'origine. Si le pool ou l'utilisateur est supprimé de View Manager, vous ne pouvez pas utiliser le disque persistant pour recréer un poste de travail de clone lié.

En modifiant le pool et l'utilisateur, vous pouvez utiliser le disque persistant détaché pour recréer un poste de travail dans le nouveau pool. Le poste de travail est affecté au nouvel utilisateur.

Vous pouvez sélectionner un nouveau pool, un nouvel utilisateur, ou les deux.

Prérequis

- Vérifiez que le pool ou l'utilisateur du disque persistant a été supprimé de View Manager.
- Vérifiez que le nouveau pool utilise le même système d'exploitation que le pool dans lequel le disque persistant a été créé.

Procédure

1 Dans View Administrator, cliquez sur **[Inventory (Inventaire)] > [Persistent Disks (Disques persistants)]**

2 Sélectionnez le disque persistant pour lequel l'utilisateur ou le pool a été supprimé.

3 Cliquez sur **[Edit (Modifier)]** .

4 (Facultatif) Sélectionnez un pool de clone lié dans la liste.

5 (Facultatif) Sélectionnez un utilisateur pour le disque persistant.

Vous pouvez rechercher votre Active Directory pour le domaine et le nom d'utilisateur.

Suivant

Recréez un poste de travail de clone lié avec le disque persistant détaché.

Recréer un poste de travail de clone lié avec un disque persistant détaché

Lorsque vous détachez un disque persistant de View Composer, le clone lié est supprimé. Vous pouvez donner l'accès utilisateur d'origine aux paramètres et informations d'utilisateur détachés en recréant le poste de travail de clone lié à partir du disque détaché.

Remarque Si vous recréez un poste de travail de clone lié dans un pool qui a atteint sa taille maximale, le poste de travail recréé est toujours ajouté au pool. La taille du pool dépasse la taille maximale spécifiée.

Si le pool ou l'utilisateur d'origine d'un disque persistant a été supprimé de View Manager, vous pouvez en affecter un nouveau au disque persistant. Reportez-vous à la section « Modifier le pool ou l'utilisateur d'un disque persistant de View Composer », page 302.

Procédure

1 Dans View Administrator, cliquez sur **[Inventory (Inventaire)] > [Persistent Disks (Disques persistants)]** .

2 Cliquez sur l'onglet **[Detached (Détaché)]** .

3 Sélectionnez le disque persistant.

Vous pouvez sélectionner plusieurs disques persistants pour recréer un poste de travail de clone lié pour chaque disque.

4 Cliquez sur **[Recreate Desktop (Recréer un poste de travail)]** .

5 Cliquez sur **[OK]** .

View Manager crée un poste de travail de clone lié pour chaque disque persistant que vous sélectionnez et ajoute le poste de travail au pool d'origine.

Les disques persistants restent sur le magasin de données sur lequel ils étaient stockés.

Restaurer un poste de travail de clone lié en important un disque persistant depuis vSphere

Si un poste de travail de clone lié devient inaccessible dans View Manager, vous pouvez restaurer le poste de travail s'il était configuré avec un disque persistant de View Composer. Vous pouvez importer le disque persistant depuis un magasin de données vSphere dans View Manager.

Vous importez le fichier disque persistant en tant que disque persistant détaché dans View Manager. Vous pouvez attacher le disque détaché à un poste de travail existant ou recréer le clone lié d'origine dans View Manager.

Procédure

1 Dans View Administrator, cliquez sur **[Inventaire]** > **[Disques persistants]** .

2 Cliquez sur l'onglet **[Détaché]** .

3 Cliquez sur **[Importer depuis vCenter]** .

4 Sélectionnez un serveur vCenter Server.

5 Sélectionnez le datacenter où se situe le fichier disque.

6 Sélectionnez un pool de clone lié dans lequel créer un nouveau poste de travail de clone lié avec le disque persistant.

7 Dans la case **[Fichier disque persistant]** , cliquez sur **[Parcourir]** , cliquez sur la flèche vers le bas et sélectionnez un magasin de données dans le menu **[Choisir un magasin de données]** .

   Vous ne pouvez pas importer un disque persistant depuis un magasin de données local. Seuls les magasins de données partagés sont disponibles.

8 Cliquez sur le nom de magasin de données pour afficher ses fichiers de stockage de disque et ses fichiers de machine virtuelle.

9 Sélectionnez le fichier disque persistant que vous voulez importer.

10 Dans la case **[Utilisateur]** , cliquez sur **[Parcourir]** , sélectionnez un utilisateur à affecter au poste de travail et cliquez sur **[OK]** .

Le fichier disque est importé dans View Manager en tant que disque persistant détaché.

Suivant

Pour restaurer le poste de travail de clone lié, vous pouvez recréer le poste de travail d'origine ou attacher le disque persistant détaché à un autre poste de travail.

Pour plus d'informations, reportez-vous à la section « Recréer un poste de travail de clone lié avec un disque persistant détaché », page 302 et « Attacher un disque persistant de View Composer à un autre poste de travail de clone lié », page 301.

Supprimer un disque persistant détaché de View Composer

Lorsque vous supprimez un disque persistant détaché, vous pouvez supprimer le disque de View Manager et le laisser sur le magasin de données ou supprimer le disque de View Manager et du magasin de données.

Procédure

1 Dans View Administrator, cliquez sur **[Inventory (Inventaire)] > [Persistent Disks (Disques persistants)]** .

2 Cliquez sur l'onglet **[Detached (Détaché)]** .

3 Sélectionnez le disque persistant.

4 Cliquez sur **[Delete (Supprimer)]** .

5 Choisissez de supprimer le disque du magasin de données ou de le laisser sur le magasin de données après sa suppression de View Manager.

Option	Description
Delete from disk (Supprimer du disque)	Après la suppression, le disque persistant n'existe plus.
Delete from View Manager only (Supprimer uniquement de View Manager)	Après la suppression, le disque persistant n'est plus accessible dans View Manager mais reste sur le magasin de données.

6 Cliquez sur **[OK]** .

Gestion de postes de travail et de pools de postes de travail 11

Dans View Administrator, vous pouvez gérer des pools de postes de travail, des postes de travail de machine virtuelle et des sessions de poste de travail.

Ce chapitre aborde les rubriques suivantes :

Gestion de pools de postes de travail

Vous pouvez modifier, désactiver et supprimer les pools de postes de travail dans View Administrator.

Modifier un pool de postes de travail

Vous pouvez modifier un pool de postes de travail existant pour configurer des paramètres comme des paramètres de pool, un nombre de postes de travail de rechange, des magasins de données et des spécifications de personnalisation.

Prérequis

Familiarisez-vous avec les paramètres de pool que vous pouvez ou non modifier après la création d'un pool. Reportez-vous à la section « Modification des paramètres dans un pool de postes de travail existant », page 306 et « Paramètres fixes dans un pool de postes de travail existant », page 307.

Procédure

1 Cliquez sur **[Inventory (Inventaire)] > [Pools]** .

2 Sélectionnez un pool.

3 Cliquez sur **[Edit (Modifier)]** .

4 Cliquez sur un onglet dans la boîte de dialogue **[Edit*pool_name*(Modifier*nom_pool*)]** et reconfigurez des options de pool.

5 Cliquez sur **[OK]** .

Modification des paramètres dans un pool de postes de travail existant

Après avoir créé un pool de postes de travail, vous pouvez modifier certains paramètres de configuration.

Tableau 11-1. Paramètres modifiables dans un pool de postes de travail existant

Onglet Configuration	Description
[Général]	Permet de modifier des options de nommage de pool.
[Paramètres de pool]	Permet de modifier des paramètres de poste de travail, tels que la règle d'alimentation de poste de travail distant, le protocole d'affichage et des paramètres Adobe Flash.
[Paramètres d'approvisionnement]	Permet de modifier des options d'approvisionnement de pool et d'ajouter des postes de travail au pool. Cet onglet n'est disponible que pour les pools automatisés.
[Paramètres de vCenter]	Permet de modifier le modèle de machine virtuelle ou l'image de base par défaut. Ajoutez ou modifiez l'instance de vCenter Server, l'hôte ou le cluster ESXi, des magasins de données et d'autres fonctions vCenter. Les nouvelles valeurs n'affectent que les machines virtuelles qui sont créées après la modification des paramètres. Les nouveaux paramètres n'affectent pas les machines virtuelles existantes. Cet onglet n'est disponible que pour les pools automatisés.
[Personnalisation client]	Permet de sélectionner des spécifications de personnalisation Sysprep. Si QuickPrep était utilisé pour personnaliser un pool de clone lié, vous pouvez modifier le domaine et le conteneur Active Directory et spécifier des scripts de mise hors tension et de post-synchronisation QuickPrep. Cet onglet n'est disponible que pour les pools automatisés.
[Stockage avancé]	Choisissez d'utiliser des snapshots NFS natifs (VAAI) et la mise en cache de l'hôte. Si vous cochez ou décochez la case **[Utiliser des snapshots NFS natifs (VAAI)]** , le nouveau paramètre n'affecte que les machines virtuelles qui sont créées après la modification des paramètres. Vous pouvez modifier des machines virtuelles existantes afin qu'elles deviennent des clones de snapshots NFS natifs en recomposant et, si nécessaire, en rééquilibrant le pool de postes de travail. Reportez-vous à la section « Utilisation de View Composer Array Integration avec la technologie de snapshot NFS natif (VAAI) », page 129. Si vous cochez ou décochez la case **[Utiliser View Storage Accelerator]** , ou si vous replanifiez lorsque les fichiers condensés de View Storage Accelerator sont régénérés, les nouveaux paramètres n'affectent pas les machines virtuelles existantes. Reportez-vous à la section « Configurer View Storage Accelerator pour des pools de postes de travail », page 167. **Remarque** Si vous cochez la case **[Utiliser View Storage Accelerator]** sur un pool de clone lié existant, et si le réplica n'était pas précédemment activé pour View Storage Accelerator, cette fonction peut ne pas prendre effet immédiatement. View Storage Accelerator ne peut pas être activé lorsque le réplica est utilisé. Vous pouvez forcer l'activation de View Storage Accelerator en recomposant le pool sur une nouvelle machine virtuelle parente.

Paramètres fixes dans un pool de postes de travail existant

Après avoir créé un pool de postes de travail, vous ne pouvez pas modifier certains paramètres de configuration.

Tableau 11-2. Paramètres fixes dans un pool de postes de travail existant

Paramètre	Description
Pool type (Type de pool)	Après avoir créé un pool automatisé, manuel ou Terminal Services, vous ne pouvez pas modifier le type de pool.
User assignment (Affectation d'utilisateur)	Vous ne pouvez pas basculer entre des affectations dédiées et des affectations flottantes.
Type of virtual machine (Type de machine virtuelle)	Vous ne pouvez pas basculer entre des postes de travail complets et des postes de travail de clone lié.
Pool ID (ID de pool)	Vous ne pouvez pas modifier l'ID de pool.
Desktop-naming and provisioning method (Méthode d'attribution de nom et d'approvisionnement de poste de travail)	Pour ajouter des postes de travail à un pool, vous devez utiliser la méthode d'approvisionnement qui a été utilisée pour créer le pool. Vous ne pouvez pas spécifier manuellement des noms de poste de travail et ensuite utiliser un mode d'attribution de nom. Si vous spécifiez des noms manuellement, vous pouvez ajouter des noms à la liste de noms de poste de travail. Si vous utilisez un mode d'attribution de nom, vous pouvez augmenter le nombre maximum de postes de travail.
vCenter settings (Paramètres de vCenter)	Vous ne pouvez pas modifier les paramètres vCenter pour des machines virtuelles existantes. Vous pouvez modifier des paramètres vCenter dans la boîte de dialogue **[Edit*pool_name*(Modifier*nom_pool*)]** , mais les valeurs n'affectent que les nouvelles machines virtuelles créées après la modification des paramètres.
View Composer persistent disks (Disques persistants de View Composer)	Vous ne pouvez pas configurer des disques persistants après la création d'un pool de clone lié sans disques persistants.
View Composer customization method (Méthode de personnalisation de View Composer)	Après avoir personnalisé un pool de clone lié avec QuickPrep ou Sysprep, vous ne pouvez passer à l'autre méthode de personnalisation lorsque vous créez ou recomposez des postes de travail dans le pool.

Modifier la taille d'un pool automatisé approvisionné par un mode d'attribution de nom

Lorsque vous approvisionnez un pool de postes de travail automatisés à l'aide d'un mode d'attribution de nom, vous pouvez augmenter ou diminuer la taille du pool en modifiant le nombre maximum de postes de travail.

Prérequis

- Vérifiez que vous avez approvisionné le pool à l'aide d'un mode d'attribution de nom. Si vous spécifiez des noms de poste de travail manuellement, reportez-vous à la section « Ajouter des postes de travail à un pool automatisé approvisionné par une liste de noms », page 308.
- Vérifiez que le pool est automatisé.

Procédure

1 Dans View Administrator, cliquez sur **[Inventaire] > [Pools]** .

2 Sélectionnez le pool et cliquez sur **[Modifier]** .

3 Cliquez sur l'onglet **[Paramètres d'approvisionnement]** .

4 Dans la zone **[Nombre max. de postes de travail]** , saisissez le nouveau nombre de postes de travail dans le pool.

Si vous augmentez la taille du pool, de nouveaux postes de travail peuvent être ajoutés au pool jusqu'à atteindre le nombre maximum.

Si vous diminuez la taille d'un pool d'affectation flottante, les postes de travail inutiles sont supprimés. Si le nombre d'utilisateurs dont la session est ouverte dans le pool est supérieur au nouveau maximum, la taille du pool diminue quand les utilisateurs ferment leur session.

Si vous diminuez la taille d'un pool d'affectation dédiée, les postes de travail non affectés sont supprimés. Si le nombre d'utilisateurs affectés à des postes de travail est supérieur au nouveau maximum, la taille du pool diminue quand vous supprimez l'affectation des utilisateurs.

Remarque Lorsque vous diminuez la taille d'un pool, le nombre réel de postes de travail peut être supérieur à la valeur **[Nombre max. de postes de travail]** si le nombre d'utilisateurs dont la session est ouverte sur ou qui sont affectés à des postes de travail est supérieur à la valeur spécifiée dans **[Nombre max. de postes de travail]** .

Ajouter des postes de travail à un pool automatisé approvisionné par une liste de noms

Pour ajouter des postes de travail à un pool automatisé approvisionné en spécifiant manuellement des noms de poste de travail, vous fournissez une autre liste de nouveaux noms de poste de travail. Cette fonction vous permet de développer un pool de postes de travail et de continuer à utiliser les conventions de dénomination de votre entreprise.

Suivez ces recommandations pour ajouter manuellement des noms de poste de travail :

- Saisissez chaque nom de poste de travail sur une ligne séparée.
- Un nom de poste de travail peut contenir 15 caractères alphanumériques maximum.
- Vous pouvez ajouter un nom d'utilisateur à chaque entrée de poste de travail. Utilisez une virgule pour séparer le nom d'utilisateur du nom de poste de travail.

Dans cet exemple, deux postes de travail sont ajoutés. Le deuxième poste de travail est associé à un utilisateur :

```
Desktop-001
Desktop-002,abccorp.com/jdoe
```

Remarque Dans un pool d'affectation flottante, vous ne pouvez pas associer des noms d'utilisateur à des noms de poste de travail. Les postes de travail ne sont pas dédiés aux utilisateurs associés. Dans un pool d'affectation flottante, tous les postes de travail qui ne sont pas actuellement utilisés restent accessibles à tout utilisateur ouvrant une session.

Prérequis

Vérifiez que vous avez créé le pool en spécifiant manuellement des noms de poste de travail. Vous ne pouvez pas ajouter de postes de travail en fournissant de nouveaux noms de poste de travail si vous avez créé le pool en fournissant un mode d'attribution de nom.

Procédure

1 Créez un fichier texte contenant la liste de noms de poste de travail supplémentaires.

Si vous prévoyez d'ajouter seulement quelques postes de travail, vous pouvez saisir les noms de poste de travail directement dans l'assistant Add Pool (Ajouter un pool). Vous n'avez pas à créer un fichier texte séparé.

2 Dans View Administrator, cliquez sur **[Inventory (Inventaire)] > [Pools]** .

3 Sélectionnez le pool à examiner.

4 Cliquez sur **[Edit (Modifier)]** .

5 Cliquez sur l'onglet **[Provisioning Settings (Paramètres d'approvisionnement)]** .

6 Cliquez sur **[Add Desktops (Ajouter des postes de travail)]** .

7 Copiez votre liste de noms de poste de travail sur la page Enter Desktop Names (Saisir des noms de poste de travail) et cliquez sur **[Next (Suivant)]** .

L'assistant Enter Desktop Names (Saisir des noms de poste de travail) affiche la liste des postes de travail et indique les erreurs de validation avec un point d'exclamation (**[!]**) rouge.

8 Corrigez les noms de poste de travail non valides.

a Placez votre curseur sur un nom non valide pour afficher le message d'erreur lié en bas de la page.

b Cliquez sur **[Back (Précédent)]** .

c Modifiez les noms incorrects et cliquez sur **[Next (Suivant)]** .

9 Cliquez sur **[Finish (Terminer)]** .

10 Cliquez sur **[OK]** .

View Manager ajoute les nouveaux postes de travail au pool.

Dans vCenter Server, vous pouvez surveiller la création des nouvelles machines virtuelles.

Dans View Administrator, vous pouvez voir les postes de travail lorsqu'ils sont ajoutés au pool en cliquant sur **[Inventory (Inventaire)] > [Pools]** ou **[Inventory (Inventaire)] > [Postes de travail]** .

Désactiver ou activer un pool de postes de travail

Lorsque vous désactivez un pool de postes de travail, le pool n'est plus disponible pour les utilisateurs et l'approvisionnement de pools est arrêté. Les utilisateurs n'ont plus accès au pool. Après avoir désactivé un pool, vous pouvez l'activer de nouveau.

Vous pouvez désactiver un pool pour empêcher les utilisateurs d'accéder à leurs postes de travail pendant que vous les préparez. Si un pool n'est plus utile, vous pouvez utiliser la fonction de désactivation pour le désactiver sans avoir à supprimer la définition de ce pool dans View Manager.

Procédure

1 Dans View Administrator, cliquez sur **[Inventory (Inventaire)] > [Pools]** .

2 Sélectionnez un pool de postes de travail et modifiez l'état du pool.

Option	Action
Disable the pool (Désactiver le pool)	Cliquez sur **[État] > [Disable Pool (Désactiver le pool)]** .
Enable the pool (Activer le pool)	Cliquez sur **[État] > [Enable Pool (Activer le pool)]** .

3 Cliquez sur **[OK]** .

Désactiver ou activer l'approvisionnement dans un pool de postes de travail

Lorsque vous désactivez l'approvisionnement dans un pool de postes de travail, View Manager interrompt l'approvisionnement des nouvelles machines virtuelles dans le pool. Après avoir désactivé l'approvisionnement, vous pouvez l'activer de nouveau.

Avant de modifier la configuration d'un pool, vous pouvez désactiver l'approvisionnement pour vous assurer qu'aucun nouveau poste de travail ne sera créé sur la base de l'ancienne configuration. Vous pouvez également désactiver l'approvisionnement pour empêcher View Manager d'utiliser un stockage supplémentaire lorsqu'un pool occupe presque tout l'espace disponible.

Lorsque l'approvisionnement est désactivé dans un pool de clone lié, View Manager empêche l'approvisionnement de nouveaux postes de travail ainsi que la personnalisation des postes de travail après recomposition ou rééquilibrage.

Procédure

1 Dans View Administrator, cliquez sur **[Inventory (Inventaire)] > [Pools]** .

2 Sélectionnez un pool de postes de travail et modifiez l'état du pool.

Option	Action
Disable provisioning (Désactiver l'approvisionnement)	Cliquez sur **[Status (État)] > [Disable Provisioning (Désactiver l'approvisionnement)]** .
Enable provisioning (Activer l'approvisionnement)	Cliquez sur **[Status (État)] > [Enable Provisioning (Activer l'approvisionnement)]** .

3 Cliquez sur **[OK]** .

Supprimer un pool de postes de travail de View Manager

Lorsque vous supprimez un pool de postes de travail de View Manager, les utilisateurs ne peuvent plus accéder aux postes de travail dans le pool.

Les utilisateurs dans des sessions actuellement actives peuvent continuer à utiliser des postes de travail de machine virtuelle complets si vous conservez les machines virtuelles dans vCenter Server. Quand les utilisateurs ferment leur session, ils ne peuvent pas accéder aux postes de travail supprimés.

Avec des postes de travail de clone lié, vCenter Server supprime toujours les machines virtuelles du disque.

Important Ne supprimez pas les machines virtuelles dans vCenter Server avant de supprimer un pool de postes de travail avec View Administrator. Cette action mettrait les composants View dans un état incohérent.

Procédure

1 Dans View Administrator, cliquez sur **[Inventaire] > [Pools]** .

2 Sélectionnez un pool de postes de travail et cliquez sur **[Supprimer]** .

3 Choisissez la façon de supprimer le pool.

Option	Description
Pool contenant des postes de travail de machine virtuelle complets	Choisissez de conserver ou de supprimer les machines virtuelles dans vCenter Server. Si vous supprimez les machines virtuelles du disque, les utilisateurs dans des sessions actives sont déconnectés de leurs postes de travail. Si vous conservez les machines virtuelles dans vCenter Server, choisissez si vous voulez que les utilisateurs dans des sessions actives restent connectés à leurs postes de travail ou si vous voulez les déconnecter.
Pool de clone lié avec des disques persistants de View Composer	Choisissez de détacher ou de supprimer les disques persistants lorsque les postes de travail sont supprimés. Dans les deux cas, vCenter Server supprime les machines virtuelles de clone lié du disque. Les utilisateurs dans des sessions actuellement actives sont déconnectés de leurs postes de travail de clone lié. Si vous détachez un disque persistant, le poste de travail de clone lié qui contenait le disque persistant peut être recréé ou le disque persistant peut être attaché à un autre poste de travail. Vous pouvez stocker des disques persistants détachés dans le même magasin de données ou un magasin de données différent. Si vous sélectionnez un magasin de données différent, vous ne pouvez pas stocker des disques persistants détachés sur un magasin de données local. Vous devez utiliser un magasin de données partagé. Vous ne pouvez détacher que les disques persistants qui ont été créés dans View 4.5 ou versions supérieures.
Pool de clone lié sans disques persistants de View Composer	vCenter Server supprime les machines virtuelles de clone lié du disque. Les utilisateurs dans des sessions actuellement actives sont déconnectés de leurs postes de travail de clone lié.

Le pool de postes de travail est supprimé de Serveur de connexion View. Si vous conservez les machines virtuelles dans vCenter Server, View Manager ne peut pas y accéder.

Lorsque vous supprimez un pool de postes de travail de View Manager, des comptes d'ordinateur de clone lié sont supprimés d'Active Directory. Des comptes de machine virtuelle complets restent dans Active Directory. Pour supprimer ces comptes, vous devez les supprimer manuellement d'Active Directory.

Lorsque vous supprimez un pool contenant des postes de travail locaux, les copies de datacenter des postes de travail sont supprimées de View Manager. Les postes de travail locaux ne fonctionnent plus lorsque les clients contactent Serveur de connexion View ou que la durée maximale sans contact avec le serveur est dépassée. Si vous choisissez de conserver les machines virtuelles complètes dans vCenter Server ou de détacher et d'enregistrer des disques persistants de View Composer, les modifications apportées par les utilisateurs sur leurs postes de travail locaux depuis la dernière réplication ou le dernier emprunt ne sont pas conservées dans les machines virtuelles ou les disques persistants.

Réduction de la bande passante Adobe Flash

Vous pouvez réduire la quantité de bande passante utilisée par le contenu Adobe Flash qui s'exécute dans des sessions de poste de travail View. Cette réduction peut améliorer la qualité globale des recherches et rendre d'autres applications exécutées sur le poste de travail plus réactives.

Configurer la qualité et la limitation d'Adobe Flash

Vous pouvez définir des modes de qualité et de limitation d'Adobe Flash pour réduire la quantité de bande passante utilisée par le contenu Adobe Flash dans des postes de travail View.

Prérequis

Familiarisez-vous avec les paramètres de qualité et de limitation d'Adobe Flash. Reportez-vous à la section « Qualité et limitation d'Adobe Flash », page 312.

Procédure

1 Dans View Administrator, cliquez sur **[Inventory (Inventaire)]** > **[Pools]** .

2 Sélectionnez un pool et cliquez sur **[Edit (Modifier)]** .

3 Cliquez sur l'onglet **[Pool Settings (Paramètres de pool)]** .

4 Sélectionnez un mode de qualité dans le menu **[Adobe Flash quality (Qualité Adobe Flash)]** .

5 Sélectionnez un mode de limitation dans le menu **[Adobe Flash throttling (Limitation d'Adobe Flash)]** .

6 Cliquez sur **[OK]** .

Remarque Les paramètres de réduction de la bande passante Adobe Flash prennent effet lorsque View Client se reconnecte au poste de travail.

Qualité et limitation d'Adobe Flash

Vous pouvez spécifier un niveau admissible maximum de qualité pour le contenu Adobe Flash qui remplace des paramètres de page Web. Si la qualité Adobe Flash pour une page Web est supérieure au niveau maximum autorisé, la qualité est réduite au maximum spécifié. Une qualité inférieure se traduit par plus d'économies de bande passante.

Pour utiliser des paramètres de réduction de bande passante Adobe Flash, Adobe Flash ne doit pas être exécuté en mode Plein écran.

Tableau 11-3 montre les paramètres de qualité du rendu Adobe Flash disponibles.

Tableau 11-3. Paramètres de qualité d'Adobe Flash

Paramètre de qualité	Description
[Do not control (Ne pas contrôler)]	La qualité est déterminée par les paramètres de page Web.
[Low (Faible)]	Ce paramètre se traduit par les meilleures économies de bande passante.
[Medium (Moyenne)]	Ce paramètre se traduit par des économies de bande passante modérées.
[High (Haute)]	Ce paramètre se traduit par des économies de bande passante moindres.

Si aucun niveau maximum de qualité n'est spécifié, le système prend la valeur par défaut **[Low (Faible)]** .

Adobe Flash utilise des services de temporisateur pour mettre à jour ce qui apparaît à l'écran à une heure donnée. La valeur d'intervalle du temporisateur Adobe Flash classique est comprise entre 4 et 50 millisecondes. En limitant, ou en prolongeant, l'intervalle, vous pouvez réduire la fréquence d'image et ainsi réduire la bande passante.

Tableau 11-4 montre les paramètres de limitation d'Adobe Flash disponibles.

Tableau 11-4. Paramètres de limitation d'Adobe Flash

Paramètre de limitation	Description
[Disabled (Désactivé)]	Aucune limitation n'est effectuée. L'intervalle du temporisateur n'est pas modifié.
[Conservative (Conservateur)]	L'intervalle du temporisateur est de 100 millisecondes. Ce paramètre correspond au plus petit nombre d'images ignorées.
[Moderate (Modéré)]	L'intervalle du temporisateur est de 500 millisecondes.
[Aggressive (Agressif)]	L'intervalle du temporisateur est de 2500 millisecondes. Ce paramètre correspond au plus grand nombre d'images ignorées.

La vitesse audio reste constante quel que soit le paramètre de limitation sélectionné.

Configurer la limitation d'Adobe Flash avec Internet Explorer dans des sessions Terminal Services

Pour s'assurer que la limitation d'Adobe Flash fonctionne avec Internet Explorer dans des sessions Terminal Services, les utilisateurs doivent activer des extensions tierce partie du navigateur.

Procédure

1 Démarrez View Client et ouvrez une session sur le poste de travail d'un utilisateur.

2 Dans Internet Explorer, cliquez sur **[Tools (Outils)] > [Internet Options (Options Internet)]** .

3 Cliquez sur l'onglet **[Advanced (Avancé)]** , sélectionnez **[Enable third-party browser extensions (Activer les extensions tierce partie du navigateur)]** , puis cliquez sur **[OK]** .

4 Redémarrez Internet Explorer.

Remplacer des paramètres de réduction de la bande passante sur le poste de travail

En utilisant le curseur de la souris sur le poste de travail, les utilisateurs peuvent remplacer les paramètres d'affichage du contenu Adobe Flash.

Procédure

1 Sur un poste de travail View, démarrez Internet Explorer et allez au contenu Adobe Flash de votre choix.

Si nécessaire, démarrez le contenu.

En fonction de la façon dont les paramètres Adobe Flash sont configurés, des images ignorées peuvent ne pas s'afficher, ou la qualité de lecture peut être mauvaise.

2 Déplacez le curseur de la souris sur le contenu Adobe Flash pendant la lecture.

La qualité d'affichage est meilleure tant que le curseur reste sur le contenu Adobe Flash.

3 Pour conserver ce niveau de qualité, double-cliquez dans le contenu Adobe Flash.

Gestion de postes de travail de machine virtuelle

Vous pouvez rechercher, gérer et supprimer des postes de travail de machine virtuelle et gérer des sessions de poste de travail.

Afficher, déconnecter, redémarrer ou envoyer des messages à des sessions actives

Vous pouvez afficher les utilisateurs activement connectés aux postes de travail View d'un pool. Vous pouvez déconnecter des utilisateurs de leurs postes de travail, forcer des utilisateurs à fermer leur session, redémarrer des sessions actives ou envoyer des messages aux postes de travail des utilisateurs.

Procédure

1 Dans View Administrator, cliquez sur **[Inventaire] > [Pool]** .

2 Double-cliquez sur un pool et cliquez sur l'onglet **[Sessions]** .

3 Sélectionnez un poste de travail.

Si vous prévoyez d'envoyer un message à des utilisateurs, vous pouvez sélectionner plusieurs postes de travail. Vous pouvez effectuer les autres opérations sur un seul poste de travail à la fois.

4 Choisissez de déconnecter, de fermer la session, de redémarrer la session ou d'envoyer un message.

Option	Description
Déconnecter la session	Déconnecte l'utilisateur du poste de travail. La session reste active. L'utilisateur peut rouvrir sa session si **[Fermeture de session automatique après la déconnexion]** est défini sur **[Jamais]** , ou si le délai spécifié après la déconnexion n'est pas dépassé. Vous pouvez configurer le paramètre **[Fermeture de session automatique après la déconnexion]** lorsque le pool est créé ou modifier le paramètre après la création du pool.
Fermer la session	Déconnecte l'utilisateur du poste de travail. La session de l'utilisateur est fermée.
Réinitialiser	Éteint le poste de travail et redémarre la session sans fermeture de session et déconnexion.
Envoyer un message	Vous permet de saisir un message affiché sur les postes de travail des utilisateurs. Vous pouvez sélectionner plusieurs postes de travail pour recevoir le message. Vous pouvez nommer le message **[Infos]** , **[Avertissement]** ou **[Erreur]** . Le message est envoyé à tous les postes de travail sélectionnés dans des sessions actives.

Affecter un poste de travail à un utilisateur

Dans un pool d'affectation dédiée, vous pouvez affecter à un utilisateur le rôle de propriétaire d'un poste de travail. Seul l'utilisateur affecté peut ouvrir une session et se connecter au poste de travail.

View Manager affecte des postes de travail à des utilisateurs dans les situations suivantes.

- Lorsque vous créez un pool et que vous sélectionnez le paramètre **[Enable automatic assignment (Activer l'affectation automatique)]** .

  REMARQUE Si vous sélectionnez le paramètre **[Enable automatic assignment (Activer l'affectation automatique)]** , vous pouvez toujours affecter manuellement des postes de travail à des utilisateurs.

- Lorsque vous créez un pool automatisé, que vous sélectionnez le paramètre **[Specify desktop names manually (Spécifier des noms de poste de travail manuellement)]** et que vous fournissez des noms d'utilisateur avec les noms de poste de travail.

Si vous ne sélectionnez aucun paramètre dans un pool d'affectation dédiée, les utilisateurs n'ont pas accès aux postes de travail. Vous devez affecter manuellement un poste de travail à chaque utilisateur.

Vous pouvez également utiliser la commande `vdmadmin` pour affecter des postes de travail à des utilisateurs. Reportez-vous à la section « Affectation de postes de travail dédiés à l'aide de l'option -L », page 475.

Prérequis

- Vérifiez que le poste de travail appartient à un pool d'affectation dédiée. Dans View Administrator, l'affectation de pool apparaît sous l'onglet Settings (Paramètres) sur la page du pool de postes de travail.
- Vérifiez que le poste de travail n'est pas emprunté pour une utilisation en mode local. Vous ne pouvez pas affecter des utilisateurs ou supprimer des affectations d'utilisateur tant que les postes de travail sont empruntés.

Procédure

1 Dans View Administrator, cliquez sur **[Inventory (Inventaire)] > [Desktops (Postes de travail)]** ou cliquez sur **[Inventory (Inventaire)] > [Pools]** , double-cliquez sur un ID de pool et sélectionnez l'onglet **[Inventory (Inventaire)]** .

2 Sélectionnez le poste de travail.

3 Cliquez sur **[More Commands (Plus de commandes)] > [Assign User (Affecter un utilisateur)]** .

4 Choisissez si vous voulez rechercher des utilisateurs ou des groupes, sélectionner un domaine et saisir une chaîne de recherche dans la zone de texte **[Name (Nom)]** ou **[Description]** .

5 Sélectionnez le nom d'utilisateur ou de groupe et cliquez sur **[OK]** .

Supprimer l'affectation d'un utilisateur d'un poste de travail dédié

Dans un pool d'affectation dédiée, vous pouvez supprimer une affectation de poste de travail à un utilisateur.

Vous pouvez également utiliser la commande `vdmadmin` pour supprimer l'affectation d'un poste de travail à un utilisateur. Reportez-vous à la section « Affectation de postes de travail dédiés à l'aide de l'option -L », page 475.

Prérequis

Vérifiez que le poste de travail n'est pas emprunté pour une utilisation en mode local. Vous ne pouvez pas affecter des utilisateurs ou supprimer des affectations d'utilisateur tant que les postes de travail sont empruntés.

Procédure

1 Dans View Administrator, cliquez sur **[Inventory (Inventaire)] > [Desktops (Postes de travail)]** ou cliquez sur **[Inventory (Inventaire)] > [Pools]** , double-cliquez sur un ID de pool et sélectionnez l'onglet **[Inventory (Inventaire)]** .

2 Sélectionnez le poste de travail.

3 Cliquez sur **[More Commands (Plus de commandes)] > [Unassign User (Supprimer l'affectation d'un utilisateur)]** .

4 Cliquez sur **[OK]** .

Le poste de travail est disponible et peut être affecté à un autre utilisateur.

Personnaliser des postes de travail existants en mode de maintenance

Après la création d'un pool de postes de travail, vous pouvez personnaliser, modifier ou tester des postes de travail individuels en les plaçant en mode de maintenance. Lorsqu'un poste de travail est en mode de maintenance, les utilisateurs ne peuvent pas y accéder.

Vous placez des postes de travail existants en mode de maintenance un par un. Vous pouvez supprimer plusieurs postes de travail du mode de maintenance en une seule opération.

Lorsque vous créez un pool, vous pouvez démarrer tous les postes de travail du pool en mode de maintenance si vous spécifiez des noms de poste de travail manuellement. Pour plus d'informations, reportez-vous à la section « Personnalisation de postes de travail en mode de maintenance », page 150.

Procédure

1 Dans View Administrator, cliquez sur **[Inventory (Inventaire)] > [Desktops (Postes de travail)]** ou cliquez sur **[Inventory (Inventaire)] > [Pools]** , double-cliquez sur un ID de pool et sélectionnez l'onglet **[Inventory (Inventaire)]** .

2 Sélectionnez un poste de travail.

3 Cliquez sur **[More Commands (Plus de commandes)] > [Enter Maintenance Mode (Passer en mode de maintenance)]** .

4 Personnalisez, modifiez ou testez le poste de travail de machine virtuelle.

5 Répétez l'Étape 2 à l'Étape 4 pour tous les postes de travail que vous voulez personnaliser.

6 Sélectionnez les postes de travail personnalisés et cliquez sur **[More Commands (Plus de commandes)] > [Exit Maintenance Mode (Quitter le mode de maintenance)]** .

Les utilisateurs peuvent accéder aux postes de travail modifiés.

Contrôler l'état du poste de travail

Vous pouvez rapidement contrôler l'état de postes de travail dans votre déploiement View à l'aide du tableau de bord de View Administrator. Par exemple, vous pouvez afficher tous les postes de travail déconnectés ou les postes de travail en mode de maintenance.

Prérequis

Familiarisez-vous avec les états de poste de travail. Reportez-vous à la section « État du poste de travail de machines virtuelles », page 316.

Procédure

1 Dans View Administrator, cliquez sur **[Dashboard (Tableau de bord)]** .

2 Dans le volet Desktop Status (État du poste de travail), développez un dossier d'état.

Option	Description
Preparing (Préparation)	Répertorie les états de poste de travail quand la machine virtuelle est approvisionnée, supprimée ou en mode de maintenance.
Problem Desktops (Postes de travail problématiques)	Répertorie les états d'erreur des postes de travail.
Prepared for use (Préparé pour l'utilisation)	Répertorie les états de poste de travail quand le poste de travail est prêt à être utilisé.

3 Recherchez l'état du poste de travail et cliquez sur le nombre hypertexte se trouvant à côté.

La page **[Desktops (Postes de travail)]** affiche tous les postes de travail avec l'état sélectionné.

Suivant

Vous pouvez cliquer sur un nom de poste de travail pour voir des détails sur ce dernier ou cliquer sur la flèche vers l'arrière de View Administrator pour revenir à la page du tableau de bord.

État du poste de travail de machines virtuelles

Les postes de travail de machine virtuelle gérés par vCenter Server peuvent se trouver dans plusieurs états d'opération et de disponibilité. Dans View Administrator, vous pouvez suivre l'état des postes de travail dans la colonne de droite de la page de la liste des postes de travail.

Tableau 11-5 montre l'état opérationnel des postes de travail de machine virtuelle affichés dans View Administrator. Un poste de travail ne peut être que dans un seul état à la fois.

Tableau 11-5. État des postes de travail de machine virtuelle gérés par vCenter Server

État	Type d'état	Description
Approvisionnement	Approvisionnement	La machine virtuelle est approvisionnée.
Erreur d'approvisionnement	Approvisionnement	Une erreur s'est produite au cours de l'approvisionnement.
Personnalisation	Approvisionnement	La machine virtuelle dans un pool automatisé est personnalisée.
Suppression	Approvisionnement	La machine virtuelle est marquée pour être supprimée. View Manager supprimera bientôt la machine virtuelle.
Mode de maintenance	Approvisionnement	La machine virtuelle est en mode de maintenance. Les utilisateurs ne peuvent pas ouvrir de session ou utiliser la machine virtuelle.

Tableau 11-5. État des postes de travail de machine virtuelle gérés par vCenter Server (suite)

État	Type d'état	Description
Attente d'Agent	État d'Agent	Serveur de connexion View attend d'établir la communication avec View Agent sur une machine virtuelle dans un pool manuel. **Remarque** Cet état est le même que l'état Personnalisation pour une machine virtuelle dans un pool automatisé.
Démarrage	État d'Agent	View Agent a démarré sur la machine virtuelle, mais d'autres services requis tels que le protocole d'affichage sont toujours en cours de démarrage. Par exemple, View Agent ne peut pas établir de connexion RDP avec des ordinateurs client tant que le démarrage de RDP n'est pas terminé. La période de démarrage de View Agent autorise d'autres processus, tels que les services de protocole, à démarrer également.
Agent inaccessible	État d'Agent	Serveur de connexion View ne peut pas établir de communication avec View Agent sur une machine virtuelle.
Erreur de configuration	État d'Agent	Le protocole d'affichage comme RDP ou PCoIP n'est pas activé.
Agent désactivé	État d'Agent	Cet état peut se produire dans deux cas. Premier cas : dans un pool de postes de travail avec le paramètre **[Supprimer ou actualiser le poste de travail à la fermeture de session]** ou **[Supprimer le poste de travail après la fermeture de session]** activé, une session de poste de travail est fermée, mais la machine virtuelle n'est pas encore actualisée ou supprimée. Second cas : le Serveur de connexion View désactive View Agent juste avant d'envoyer une demande de désactivation de la machine virtuelle. Cet état garantit qu'une nouvelle session de poste de travail ne peut pas être démarrée sur la machine virtuelle.
IP non valide	État d'Agent	Le paramètre de registre de masque de sous-réseau est configuré sur la machine virtuelle et aucune carte réseau active ne possède d'adresse IP dans la plage configurée.
L'agent doit redémarrer	État d'Agent	Un composant View a été mis à niveau et la machine virtuelle doit être redémarrée pour permettre à View Agent de fonctionner avec le composant mis à niveau.
Échec du protocole	État d'Agent	Un protocole d'affichage n'a pas démarré avant l'expiration de la période de démarrage de View Agent. **Remarque** View Administrator peut afficher des postes de travail dans un état **[Échec du protocole]** lorsqu'un protocole a échoué mais que d'autres ont démarré correctement. Par exemple, l'état **[Échec du protocole]** peut être affiché lorsqu'HTML Access a échoué mais que PCoIP et RDP fonctionnent. Dans ce cas, les postes de travail sont disponibles et les périphériques View Client peuvent y accéder via PCoIP ou RDP.
Échec du domaine	État d'Agent	La machine virtuelle a rencontré un problème pour atteindre le domaine. Le serveur de domaine n'était pas accessible ou l'authentification de domaine a échoué.
Approvisionné	Disponibilité	La machine virtuelle est hors tension ou interrompue.
Disponible	Disponibilité	La machine virtuelle est sous tension et prête pour une connexion active. Dans un pool dédié, la machine virtuelle est affectée à un utilisateur et démarre quand l'utilisateur ouvre une session.
Emprunté	État de session	La machine virtuelle d'un poste de travail local est empruntée.
Connecté	État de session	La machine virtuelle est dans une session active et a une connexion à distance active vers un client View.
Déconnecté	État de session	La machine virtuelle est dans une session active, mais elle est déconnectée du client View.

Tableau 11-5. État des postes de travail de machine virtuelle gérés par vCenter Server (suite)

État	Type d'état	Description
Utilisateur non affecté connecté	État de session	La session d'un utilisateur différent de l'utilisateur affecté est ouverte sur une machine virtuelle dans un pool dédié. Par exemple, cet état peut se produire si un administrateur démarre vSphere Client, ouvre une console sur la machine virtuelle, puis ouvre une session.
Utilisateur non affecté déconnecté	État de session	Un utilisateur différent de l'utilisateur affecté a une session ouverte sur et est déconnecté d'une machine virtuelle dans un pool dédié.
Déjà utilisé	État de session	Dans un pool de postes de travail avec le paramètre **[Supprimer ou actualiser le poste de travail à la fermeture de session]** ou **[Supprimer le poste de travail après la fermeture de session]** activé, il n'y a aucune session active sur la machine virtuelle, mais la session n'a pas été fermée. Cette condition peut se produire si la machine virtuelle s'arrête de façon inattendue ou si l'utilisateur réinitialise le poste de travail lors d'une session active. Par défaut, lorsqu'une machine virtuelle est dans cet état, View empêche tous les autres périphériques View Client d'accéder au poste de travail.
Emprunté	Mode local	La machine virtuelle est empruntée pour une utilisation en mode local.
Emprunt en cours	Mode local	La machine virtuelle est en cours d'emprunt pour une utilisation en mode local.
Restitué	Mode local	Une machine virtuelle qui a été empruntée pour une utilisation en mode local est maintenant de nouveau restituée.
Restitution en cours	Mode local	Une machine virtuelle empruntée pour une utilisation en mode local est en cours de restitution à la machine virtuelle vCenter Server dans le datacenter.
Réplication en cours	Mode local	La machine virtuelle est empruntée pour une utilisation en mode local et réplique des données pour la machine virtuelle vCenter Server dans le datacenter.
Restauration	Mode local	La machine virtuelle empruntée pour une utilisation en mode local est en cours de restauration. La machine virtuelle de poste de travail local est ignorée et est en cours de déverrouillage sur la version vCenter Server de la machine virtuelle.
En cours	Divers	La machine virtuelle est dans un état de transition lors d'une opération de maintenance.
Inconnu	Divers	La machine virtuelle est dans un état inconnu.
Erreur	Divers	Une erreur inconnue s'est produite dans la machine virtuelle.
–	Divers	Une panne s'est produite lorsque la machine virtuelle était dans l'un des états précédents.

Quand un poste de travail est dans un état particulier, il peut être sujet à d'autres conditions. View Administrator affiche ces conditions comme des suffixes à l'état du poste de travail. Par exemple, View Administrator peut afficher l'état `Personnalisation (manquant)`.

Tableau 11-6 montre ces conditions supplémentaires.

Tableau 11-6. Conditions d'état du poste de travail

Condition	Description
Manquant	La machine virtuelle est manquante dans vCenter Server. Généralement, la machine virtuelle a été supprimée dans vCenter Server, mais la configuration View LDAP a toujours un enregistrement du poste de travail.
Tâche arrêtée	Une opération de View Composer, telle qu'une actualisation, une recomposition ou un rééquilibrage, a été arrêtée. Pour plus d'informations sur le dépannage d'une opération de recomposition, reportez-vous à la section « Corriger une recomposition échouée », page 296. Pour plus d'informations sur les états d'erreur de View Composer, reportez-vous à la section « Erreurs d'approvisionnement de View Composer », page 456. La condition `Tâche arrêtée` s'applique à toutes les machines virtuelles qui ont été sélectionnées pour l'opération, mais sur lesquelles l'opération n'a pas encore démarré. Les machines virtuelles dans le pool qui ne sont pas sélectionnées pour l'opération ne sont pas placées dans la condition `Tâche arrêtée`.

Un état de poste de travail peut être sujet à deux conditions, `(manquant, tâche arrêtée)`, si une tâche de View Composer a été arrêtée et que la machine virtuelle est manquante dans vCenter Server.

Supprimer des postes de travail de View Manager

Lorsque vous supprimez des postes de travail de View Manager, les utilisateurs ne peuvent plus accéder aux postes de travail.

Les utilisateurs dans des sessions actuellement actives peuvent continuer à utiliser des postes de travail de machine virtuelle complets si vous conservez les machines virtuelles dans vCenter Server. Quand les utilisateurs ferment leur session, ils ne peuvent pas accéder aux postes de travail supprimés.

Avec des postes de travail de clone lié, vCenter Server supprime toujours les machines virtuelles du disque.

Remarque Ne supprimez pas les machines virtuelles dans vCenter Server avant de supprimer des postes de travail avec View Administrator. Cette action mettrait les composants View dans un état incohérent.

Procédure

1 Dans View Administrator, cliquez sur **[Inventaire] > [Postes de travail]** .

2 Sélectionnez un ou plusieurs postes de travail et cliquez sur **[Supprimer]** .

3 Choisissez la façon de supprimer les postes de travail.

Option	Description
Pool contenant des postes de travail de machine virtuelle complets	Choisissez de conserver ou de supprimer les machines virtuelles dans vCenter Server. Si vous supprimez les machines virtuelles du disque, les utilisateurs dans des sessions actives sont déconnectés de leurs postes de travail. Si vous conservez les machines virtuelles dans vCenter Server, choisissez si vous voulez que les utilisateurs dans des sessions actives restent connectés à leurs postes de travail ou si vous voulez les déconnecter.
Pool de clone lié avec des disques persistants de View Composer	Choisissez de détacher ou de supprimer les disques persistants lorsque les postes de travail sont supprimés. Dans les deux cas, vCenter Server supprime les machines virtuelles de clone lié du disque. Les utilisateurs dans des sessions actuellement actives sont déconnectés de leurs postes de travail de clone lié. Si vous détachez un disque persistant, le poste de travail de clone lié qui contenait le disque persistant peut être recréé ou le disque persistant peut être attaché à un autre poste de travail. Vous pouvez stocker des disques persistants détachés dans le même magasin de données ou un magasin de données différent. Si vous sélectionnez un magasin de données différent, vous ne pouvez pas stocker des disques persistants détachés sur un magasin de données local. Vous devez utiliser un magasin de données partagé. Vous ne pouvez détacher que les disques persistants qui ont été créés dans View 4.5 ou versions supérieures.
Pool de clone lié sans disques persistants de View Composer	vCenter Server supprime les machines virtuelles de clone lié du disque. Les utilisateurs dans des sessions actuellement actives sont déconnectés de leurs postes de travail de clone lié.

Les postes de travail sont supprimés de Serveur de connexion View. Si vous conservez les machines virtuelles dans vCenter Server, View Manager ne peut pas y accéder.

Lorsque vous supprimez des postes de travail de View Manager, des comptes d'ordinateur de clone lié sont supprimés d'Active Directory. Des comptes de machine virtuelle complets restent dans Active Directory. Pour supprimer ces comptes, vous devez les supprimer manuellement d'Active Directory.

Lorsque vous supprimez des postes de travail locaux, les copies de datacenter des postes de travail sont supprimées de View Manager. Les postes de travail locaux ne fonctionnent plus lorsque les clients contactent Serveur de connexion View ou que la durée maximale sans contact avec le serveur est dépassée. Si vous choisissez de conserver les machines virtuelles complètes dans vCenter Server ou de détacher et d'enregistrer des disques persistants de View Composer, les modifications apportées par les utilisateurs sur leurs postes de travail locaux depuis la dernière réplication ou le dernier emprunt ne sont pas conservées dans les machines virtuelles ou les disques persistants.

Exporter des informations de View vers des fichiers externes

Dans View Administrator, vous pouvez exporter des informations de tableau View vers des fichiers externes. Vous pouvez exporter les tableaux qui répertorient des utilisateurs et des groupes, des pools, des postes de travail, des disques persistants de View Composer, des applications ThinApp, des événements et des sessions VDI. Vous pouvez afficher et gérer les informations dans une feuille de calcul ou un autre outil.

Par exemple, vous pouvez collecter des informations sur des postes de travail gérés par plusieurs instances de View Connection Server ou groupes d'instances de View Connection Server répliquées. Vous pouvez exporter le tableau **[Desktops (Postes de travail)]** à partir de chaque interface de View Administrator et l'afficher dans une feuille de calcul.

Lorsque vous exportez un tableau View Administrator, il est enregistré sous forme de fichier `cvs` séparé par des virgules. Cette fonction exporte l'ensemble du tableau, pas des pages individuelles.

Procédure

1 Dans View Administrator, affichez le tableau que vous voulez exporter.

Par exemple, cliquez sur **[Inventory (Inventaire)] > [Desktops (Postes de travail)]** pour afficher le tableau de postes de travail.

2 Cliquez sur l'icône **[Export (Exporter)]** dans le coin supérieur droit du tableau.

Lorsque vous pointez votre souris sur l'icône, elle affiche l'infobulle `Export table contents (Exporter le contenu du tableau)`.

3 Saisissez un nom de fichier pour le fichier `csv` dans la boîte de dialogue Select location for download (Sélectionner un emplacement pour le téléchargement).

Le nom de fichier par défaut est `global_table_data_export.csv`.

4 Recherchez un emplacement pour stocker le fichier.

5 Cliquez sur **[Save (Enregistrer)]** .

Suivant

Ouvrez une feuille de calcul ou un autre outil pour voir le fichier `csv`.

Gestion d'ordinateurs physiques et de serveurs Terminal Server 12

Dans View Administrator, vous pouvez ajouter, supprimer et désinscrire des postes de travail View non gérés par vCenter Server. Les sources de postes de travail non gérées comportent des machines virtuelles non gérées par vCenter Server, des ordinateurs physiques, des PC lame et des sources Microsoft Terminal Services.

Remarque Lorsque vous reconfigurez un paramètre qui affecte une source de postes de travail non gérée, un maximum de 10 minutes peut être nécessaire pour que le nouveau paramètre prenne effet. Par exemple, si vous modifiez le mode de sécurité des messages dans Global Settings (Paramètres généraux) ou que vous modifiez le paramètre Automatically logoff after disconnect (Fermeture de session automatique après la déconnexion) pour un pool, View Manager peut prendre jusqu'à 10 minutes pour reconfigurer les sources de postes de travail non gérées affectées.

Ce chapitre aborde les rubriques suivantes :

Ajouter une source de postes de travail non gérée à un pool

Vous pouvez augmenter la taille d'un pool de postes de travail manuel qui utilise des sources de postes de travail non gérées en ajoutant des sources de postes de travail au pool.

Prérequis

Vérifiez que View Agent est installé sur la source de postes de travail non gérée. Reportez-vous à la section « Installer View Agent sur une source de postes de travail non gérée », page 62.

Procédure

1 Dans View Administrator, cliquez sur **[Inventory (Inventaire)] > [Pools]** .

2 Dans la colonne de gauche du tableau Pools, cliquez sur l'ID de pool du pool manuel.

3 Sous l'onglet **[Inventory (Inventaire)]** , cliquez sur **[Add (Ajouter)]** .

4 Sélectionnez les sources de postes de travail dans la fenêtre Add Desktops (Ajouter des postes de travail) et cliquez **[OK]** .

View Manager ajoute la source de postes de travail au pool.

Supprimer une source de postes de travail non gérée d'un pool

Vous pouvez réduire la taille d'un pool de postes de travail manuel qui utilise des sources de postes de travail non gérées en supprimant des sources de postes de travail du pool.

Procédure

1 Dans View Administrator, cliquez sur **[Inventory (Inventaire)]** > **[Pools]** .

2 Double-cliquez sur un ID de pool et sélectionnez l'onglet **[Inventory (Inventaire)]** .

3 Sélectionnez les sources de postes de travail à supprimer.

4 Cliquez sur **[Remove (Supprimer)]** .

5 Si des utilisateurs ont ouvert une session sur les postes de travail non gérés, choisissez de terminer les sessions ou de les laisser actives.

Option	Description
Leave active (Laisser actives)	Les sessions actives le resteront jusqu'à ce que l'utilisateur ferme sa session. View Connection Server ne garde pas de trace de ces sessions.
Terminate (Mettre fin)	Les sessions actives sont terminées immédiatement.

6 Cliquez sur **[OK]** .

View Manager supprime les sources de postes de travail du pool.

Supprimer un pool contenant des postes de travail non gérés

Lorsque vous supprimez un pool de postes de travail contenant des sources de postes de travail non gérées, le pool est supprimé de View Manager.

Procédure

1 Dans View Administrator, cliquez sur **[Inventory (Inventaire)]** > **[Pools]** .

2 Sélectionnez un pool de postes de travail non géré et cliquez sur **[Delete (Supprimer)]** .

3 Si des utilisateurs ont ouvert une session sur les postes de travail non gérés, choisissez de terminer les sessions ou de les laisser actives.

Option	Description
Leave active (Laisser actives)	Les sessions actives le resteront jusqu'à ce que l'utilisateur ferme sa session. View Connection Server ne garde pas de trace de ces sessions.
Terminate (Mettre fin)	Les sessions actives sont terminées immédiatement.

4 Cliquez sur **[OK]** .

Le pool de postes de travail non géré est supprimé de View Manager. View Manager ne supprime pas les informations d'inscription des sources de postes de travail non gérées qui appartiennent au pool.

Pour supprimer les sources de postes de travail non gérées de View Manager, vous devez les désinscrire. Reportez-vous à la section « Désinscrire une source de postes de travail non gérée », page 325.

Désinscrire une source de postes de travail non gérée

Toutes les sources de postes de travail gérées par vCenter Server sont inscrites lorsque vous installez View Agent. Vous ne pouvez désinscrire que les sources de postes de travail non gérées.

Les sources de postes de travail non gérées comportent des machines virtuelles non gérées par vCenter Server, des ordinateurs physiques, des PC lame et des sources Terminal Services.

Lorsque vous désinscrivez une source de postes de travail, cette dernière devient indisponible dans View Manager. Pour qu'une source soit de nouveau disponible, réinstallez View Agent dans la source de postes de travail.

Prérequis

Vérifiez que les sources de postes de travail que vous souhaitez désinscrire ne sont pas utilisées dans d'autres pools de postes de travail.

Procédure

1 Cliquez sur **[View Configuration (Configuration de View)] > [Registered desktop sources (Sources de postes de travail inscrites)]** .

2 Sélectionnez le type de source de postes de travail non gérée et cliquez sur **[Details (Détails)]**

3 Sélectionnez la source de postes de travail à désinscrire et cliquez sur **[Unregister (Désinscrire)]** .

Vous ne pouvez sélectionner que les sources de postes de travail qui ne sont pas utilisées par un pool de postes de travail.

4 Cliquez sur **[OK]** pour confirmer que vous voulez désinscrire la source de postes de travail.

La source de postes de travail est désinscrite et n'est plus disponible.

État du poste de travail d'ordinateurs physiques et de serveurs Terminal Server

Des sources de postes de travail qui sont des ordinateurs physiques, des serveurs Terminal Server ou des machines virtuelles non gérés par vCenter Server peuvent se trouver dans plusieurs états d'opération et de disponibilité. Dans View Administrator, vous pouvez suivre l'état des postes de travail dans la colonne de droite de la page de la liste des postes de travail.

Tableau 12-1 montre l'état opérationnel des postes de travail d'ordinateur physique et de serveur Terminal Server affichés dans View Administrator. Un poste de travail ne peut être que dans un seul état à la fois.

Tableau 12-1. État de postes de travail qui sont des ordinateurs physiques ou des serveurs Terminal Server

État	Type d'état	Description
Waiting for Agent (Attente d'Agent)	État d'Agent	View Connection Server attend de recevoir la première demande de View Agent sur un poste de travail d'ordinateur physique ou de serveur Terminal Server.
Agent not reachable (Agent inaccessible)	État d'Agent	View Connection Server ne peut pas établir de communication avec View Agent sur le poste de travail. L'ordinateur source de postes de travail peut être hors tension.
Configuration error (Erreur de configuration)	État d'Agent	Le protocole d'affichage comme RDP n'est pas activé, un serveur Terminal Server n'est pas activé ou un autre protocole n'est pas activé.
Available (Disponible)	Disponibilité	L'ordinateur source de postes de travail est sous tension et le poste de travail est prêt pour une connexion active. Dans un pool dédié, le poste de travail est affecté à un utilisateur. Le poste de travail démarre quand l'utilisateur ouvre une session.

Tableau 12-1. État de postes de travail qui sont des ordinateurs physiques ou des serveurs Terminal Server (suite)

État	Type d'état	Description
Connected (Connecté)	État de session	Le poste de travail est dans une session active et a une connexion à distance active vers un client View.
Disconnected (Déconnecté)	État de session	Le poste de travail est dans une session active, mais il est déconnecté du client View.
–	Divers	Une panne s'est produite lorsque le poste de travail était dans l'un des états précédents.

Gestion d'applications ThinApp dans View Administrator

13

Vous pouvez utiliser View Administrator pour distribuer et gérer des applications livrées avec VMware ThinApp™. La gestion d'applications ThinApp dans View Administrator implique la capture et le stockage de packages d'applications, l'ajout d'applications ThinApp à View Administrator et l'affectation d'applications ThinApp à des postes de travail et des pools.

Vous devez posséder une licence pour utiliser la fonction de gestion ThinApp dans View Administrator.

IMPORTANT Si, au lieu de distribuer des applications ThinApp en les affectant à des postes de travail et des pools, vous préférez affecter des applications ThinApp à des utilisateurs et des groupes Active Directory, vous pouvez utiliser VMware Horizon Workspace.

Ce chapitre aborde les rubriques suivantes :

Configuration requise de View pour des applications ThinApp

Lors de la capture et du stockage d'applications ThinApp qui seront distribuées sur des postes de travail View dans View Administrator, vous devez satisfaire certaines exigences.

- Vous devez assembler vos applications sous forme de packages MSI (Microsoft Installation).
- Vous devez utiliser ThinApp version 4.6 ou supérieure pour créer ou reconditionner les packages MSI.
- Vous devez stocker les packages MSI sur un partage de réseau Windows qui réside dans un domaine Active Directory accessible pour votre hôte de View Connection Server et vos postes de travail View. Le serveur de fichiers doit prendre en charge l'authentification et les autorisations de fichiers basées sur des comptes d'ordinateur.
- Vous devez configurer les autorisations de fichier et de partage sur le partage de réseau qui héberge les packages MSI pour donner un accès en lecture aux ordinateurs de domaine du groupe Active Directory intégré. Si vous prévoyez de distribuer des applications ThinApp à des contrôleurs de domaine, vous devez également donner un accès en lecture aux contrôleurs de domaine du groupe Active Directory intégré.

- Pour autoriser les utilisateurs à accéder à des packages d'applications ThinApp continues, vous devez définir l'autorisation NTFS du partage de réseau hébergeant les packages d'applications ThinApp sur `Read&Execute (Lire et exécuter)` pour les utilisateurs.
- Vérifiez qu'un espace de noms disjoint n'empêche pas les ordinateurs d'un membre du domaine d'accéder au partage réseau hébergeant les packages MSI. Un espace de noms disjoint se produit lorsqu'un nom de domaine Active Directory diffère de l'espace de noms DNS utilisé par les machines de ce domaine. Pour plus d'informations, consultez l'article 1023309 de la base de connaissances de VMWare.
- Pour exécuter des applications ThinApp continues sur des postes de travail View, les utilisateurs doivent avoir accès au partage de réseau qui héberge les packages MSI.

Capture et stockage de packages d'applications

ThinApp permet de virtualiser des applications en découplant une application du système d'exploitation sous-jacent et de ses bibliothèques et infrastructure et en regroupant l'application dans un seul fichier exécutable appelé package d'application.

Pour gérer des applications ThinApp dans View Administrator, vous devez utiliser l'assistant ThinApp Setup Capture pour capturer et assembler vos applications au format MSI et stocker les packages MSI dans un référentiel d'applications.

Un référentiel d'applications est un partage de réseau Windows. Vous utilisez View Administrator pour enregistrer le partage de réseau en tant que référentiel d'applications. Vous pouvez enregistrer plusieurs référentiels d'applications.

Remarque Si vous possédez plusieurs référentiels d'applications, vous pouvez utiliser des solutions tierces pour gérer l'équilibrage de charge et la disponibilité. View ne comporte pas de solutions d'équilibrage de charge ou de disponibilité.

Pour plus d'informations sur les fonctions d'application ThinApp et sur la façon d'utiliser l'assistant ThinApp Setup Capture, consultez les guides *Introduction to VMware ThinApp (Présentation de VMware ThinApp)* et *ThinApp User's Guide (Guide de l'utilisateur de ThinApp)*.

1 Assembler vos applications page 329

Vous utilisez l'assistant ThinApp Setup Capture pour capturer et assembler vos applications.

2 Créer un partage de réseau Windows page 329

Vous devez créer un partage de réseau Windows pour héberger les packages MSI qui sont distribués à des postes de travail et des pools View dans View Administrator.

3 Enregistrer un référentiel d'applications page 330

Vous devez enregistrer le partage de réseau Windows qui héberge vos packages MSI sous forme de référentiel d'applications dans View Administrator.

4 Ajouter des applications ThinApp à View Administrator page 330

Vous ajoutez des applications ThinApp à View Administrator en analysant un référentiel d'applications et en sélectionnant des applications ThinApp. Après avoir ajouté une application ThinApp à View Administrator, vous pouvez l'affecter à des postes de travail et des pools.

5 Créer un modèle d'application ThinApp page 331

Vous pouvez créer un modèle dans View Administrator pour spécifier un groupe d'applications ThinApp. Vous pouvez utiliser des modèles pour grouper des applications par fonction, par fournisseur ou par tout autre groupement logique approprié à votre entreprise.

Assembler vos applications

Vous utilisez l'assistant ThinApp Setup Capture pour capturer et assembler vos applications.

Prérequis

- Téléchargez le logiciel ThinApp sur le site http://www.vmware.com/fr/products/thinapp et installez-le sur un ordinateur sain. View prend en charge ThinApp version 4.6 et supérieure.
- Familiarisez-vous avec la configuration du logiciel ThinApp et les instructions sur la conception des applications dans le guide *ThinApp User's Guide (Guide de l'utilisateur de ThinApp)*.

Procédure

1 Démarrez l'assistant ThinApp Setup Capture et suivez les invites.

2 Lorsque l'assistant ThinApp Setup Capture vous invite à indiquer un emplacement pour le projet, sélectionnez **[Build MSI package (Créer un package MSI)]** .

3 Si vous prévoyez d'utiliser en continu l'application sur des postes de travail View, définissez la propriété MSIStreaming sur 1 dans le fichier `package.ini`.

```
MSIStreaming=1
```

L'assistant ThinApp Setup Capture encapsule l'application, tous les composants nécessaires pour exécuter l'application et l'application elle-même dans un package MSI.

Suivant

Créez un partage de réseau Windows pour stocker les packages MSI.

Créer un partage de réseau Windows

Vous devez créer un partage de réseau Windows pour héberger les packages MSI qui sont distribués à des postes de travail et des pools View dans View Administrator.

Prérequis

- Utilisez l'assistant ThinApp Capture Setup pour assembler les applications.
- Vérifiez que le partage réseau satisfait les exigences View en termes de stockage des applications ThinApp. Reportez-vous à la section « Configuration requise de View pour des applications ThinApp », page 327 pour plus d'informations.

Procédure

1 Créez un dossier partagé sur un ordinateur dans un domaine Active Directory accessible à votre hôte de View Connection Server et vos postes de travail View.

2 Configurez les autorisations de fichier et de partage sur le dossier partagé pour donner un accès en lecture aux ordinateurs de domaine du groupe Active Directory intégré.

3 Si vous prévoyez d'affecter des applications ThinApp à des contrôleurs de domaine, donnez un accès en lecture aux contrôleurs de domaine du groupe Active Directory intégré.

4 Si vous prévoyez d'utiliser des packages d'applications ThinApp continues, définissez l'autorisation NTFS du partage de réseau hébergeant les packages d'applications ThinApp sur `Read&Execute (Lire et exécuter)` pour les utilisateurs.

5 Copiez vos packages MSI dans le dossier partagé.

Suivant

Enregistrez le partage de réseau Windows en tant que référentiel d'applications dans View Administrator.

Enregistrer un référentiel d'applications

Vous devez enregistrer le partage de réseau Windows qui héberge vos packages MSI sous forme de référentiel d'applications dans View Administrator.

Vous pouvez enregistrer plusieurs référentiels d'applications.

Prérequis

Créez un partage de réseau Windows.

Procédure

1 Dans View Administrator, sélectionnez **[View Configuration (Configuration de View)] > [ThinApp Configuration (Configuration d'application ThinApp)]** et cliquez sur **[Add Repository (Ajouter un référentiel)]** .

2 Saisissez un nom d'affichage pour le référentiel d'applications dans la zone de texte **[Display name (Nom d'affichage)]** .

3 Saisissez le chemin vers le partage de réseau Windows qui héberge vos packages d'applications dans la zone de texte **[Share path (Chemin de partage)]** .

Le chemin du partage de réseau doit être au format *ServerComputerName**ShareName* où *ServerComputerName* est le nom DNS de l'ordinateur serveur. Ne spécifiez pas d'adresse IP.

Par exemple : `\\server.domain.com\MSIPackages`

4 Cliquez sur **[Save (Enregistrer)]** pour enregistrer le référentiel d'applications avec View Administrator.

Ajouter des applications ThinApp à View Administrator

Vous ajoutez des applications ThinApp à View Administrator en analysant un référentiel d'applications et en sélectionnant des applications ThinApp. Après avoir ajouté une application ThinApp à View Administrator, vous pouvez l'affecter à des postes de travail et des pools.

Prérequis

Enregistrez un référentiel d'applications avec View Administrator.

Procédure

1 Dans View Administrator, sélectionnez **[Inventory (Inventaire)] > [ThinApps (Applications ThinApp)]** .

2 Sous l'onglet **[Summary (Résumé)]** , cliquez sur **[Scan New ThinApps (Analyser de nouvelles applications ThinApp)]** .

3 Sélectionnez un référentiel d'applications et un dossier à analyser et cliquez sur **[Next (Suivant)]** .

Si le référentiel d'applications contient des sous-dossiers, vous pouvez développer le dossier racine et sélectionner un sous-dossier.

4 Sélectionnez les applications ThinApp que vous voulez ajouter à View Administrator.

Vous pouvez appuyer sur Ctrl+clic ou Maj+clic pour sélectionner plusieurs applications ThinApp.

5 Cliquez sur **[Scan (Analyser)]** pour commencer à analyser les packages MSI que vous avez sélectionnés.

Vous pouvez cliquer sur **[Stop Scan (Arrêter l'analyse)]** si vous devez arrêter l'analyse.

View Administrator signale l'état de chaque opération d'analyse et le nombre d'applications ThinApp qui ont été ajoutées à View Administrator. Si vous sélectionnez une application qui est déjà dans View Administrator, elle n'est pas ajoutée de nouveau.

6 Cliquez sur **[Finish (Terminer)]** .

Les nouvelles applications ThinApp apparaissent sous l'onglet **[Summary (Résumé)]** .

Suivant

(Facultatif) Créez des modèles d'application ThinApp.

Créer un modèle d'application ThinApp

Vous pouvez créer un modèle dans View Administrator pour spécifier un groupe d'applications ThinApp. Vous pouvez utiliser des modèles pour grouper des applications par fonction, par fournisseur ou par tout autre groupement logique approprié à votre entreprise.

Avec des modèles d'application ThinApp, vous pouvez rationaliser la distribution de plusieurs applications. Lorsque vous affectez un modèle d'application ThinApp à un poste de travail ou à un pool, View Administrator installe toutes les applications qui se trouvent actuellement dans le modèle.

La création de modèles d'application ThinApp est facultative.

Remarque Si vous ajoutez une application à un modèle d'application ThinApp après avoir affecté un modèle à un poste de travail ou à un pool, View Administrator n'affecte pas automatiquement la nouvelle application au poste de travail ou au pool. Si vous supprimez une application d'un modèle d'application ThinApp qui était précédemment affecté à un poste de travail ou à un pool, l'application reste affectée au poste de travail ou au pool.

Prérequis

Ajoutez des applications ThinApp sélectionnées à View Administrator.

Procédure

1 Dans View Administrator, sélectionnez **[Inventory (Inventaire)] > [ThinApps (Applications ThinApp)]** et cliquez sur **[New Template (Nouveau modèle)]** .

2 Saisissez un nom pour le modèle et cliquez sur **[Add (Ajouter)]** .

Toutes les applications ThinApp disponibles apparaissent dans le tableau.

3 Pour rechercher une application ThinApp particulière, saisissez le nom de l'application dans la zone de texte **[Find (Rechercher)]** et cliquez sur **[Find (Rechercher)]** .

4 Sélectionnez les applications ThinApp que vous voulez inclure dans le modèle et cliquez sur **[Add (Ajouter)]** .

Vous pouvez appuyer sur Ctrl+clic ou Maj+clic pour sélectionner plusieurs applications.

5 Cliquez sur **[OK]** pour enregistrer le modèle.

Affectation d'applications ThinApp à des postes de travail et des pools

Pour installer une application ThinApp sur un poste de travail View, vous utilisez View Administrator pour affecter l'application ThinApp à un poste de travail ou à un pool.

Lorsque vous affectez une application ThinApp à un poste de travail, View Administrator commence à installer l'application sur le poste de travail quelques minutes plus tard. Lorsque vous affectez une application ThinApp à un pool, View Administrator commence à installer l'application la première fois qu'un utilisateur ouvre une session sur un poste de travail dans le pool.

Streaming (En continu) View Administrator installe un raccourci vers l'application ThinApp sur le poste de travail. Le raccourci pointe vers l'application ThinApp sur le partage de réseau qui héberge le référentiel. Les utilisateurs doivent avoir accès au partage de réseau pour exécuter des applications ThinApp continues.

Full (Complète) View Administrator installe l'application ThinApp complète sur le système de fichiers local.

Le temps nécessaire à l'installation d'une application ThinApp dépend de la taille de l'application.

IMPORTANT Vous pouvez affecter des applications ThinApp à des postes de travail et des pools qui ont uniquement des sources de machine virtuelle. Vous ne pouvez pas affecter des applications ThinApp à des serveurs Terminal Server, des PC lame ou des PC traditionnels.

- Meilleures pratiques pour l'affectation d'applications ThinApp page 333

  Suivez des meilleures pratiques lorsque vous affectez des applications ThinApp à des postes de travail et des pools.

- Affecter une application ThinApp à plusieurs postes de travail page 333

  Vous pouvez affecter une application ThinApp particulière à un ou plusieurs postes de travail.

- Affecter plusieurs applications ThinApp à un poste de travail page 334

  Vous pouvez affecter une ou plusieurs applications ThinApp à un poste de travail particulier.

- Affecter une application ThinApp à plusieurs pools page 335

  Vous pouvez affecter une application ThinApp particulière à un ou plusieurs pools.

- Affecter plusieurs applications ThinApp à un pool page 336

  Vous pouvez affecter une ou plusieurs applications ThinApp à un pool particulier.

- Affecter un modèle d'application ThinApp à un poste de travail ou à un pool page 337

  Vous pouvez rationaliser la distribution de plusieurs applications ThinApp en affectant un modèle d'application ThinApp à un poste de travail ou à un pool.

- Consulter des affectations d'application ThinApp page 338

  Vous pouvez consulter tous les postes de travail et pools auxquels une application ThinApp particulière est actuellement affectée. Vous pouvez également consulter toutes les applications ThinApp affectées à un poste de travail ou un pool particulier.

- Afficher des informations de package MSI page 339

  Après avoir ajouté une application ThinApp à View Administrator, vous pouvez afficher des informations sur son package MSI.

Meilleures pratiques pour l'affectation d'applications ThinApp

Suivez des meilleures pratiques lorsque vous affectez des applications ThinApp à des postes de travail et des pools.

- Pour installer une application ThinApp sur un poste de travail particulier, affectez l'application au poste de travail. Si vous utilisez une convention de dénomination commune pour vos postes de travail, vous pouvez utiliser des affectations de postes de travail pour distribuer rapidement des applications à tous les postes de travail qui utilisent cette convention de dénomination.
- Pour installer une application ThinApp sur tous les postes de travail dans un pool, affectez l'application au pool. Si vous organisez vos pools par service ou par type d'utilisateur, vous pouvez utiliser des affectations de pools pour distribuer rapidement des applications à des services ou des utilisateurs spécifiques. Par exemple, si vous avez un pool pour les utilisateurs de votre service comptabilité, vous pouvez distribuer la même application à tous les utilisateurs de votre service comptabilité en affectant l'application au pool comptabilité.
- Pour rationaliser la distribution de plusieurs applications ThinApp, incluez les applications dans un modèle d'application ThinApp. Lorsque vous affectez un modèle d'application ThinApp à un poste de travail ou à un pool, View Administrator installe toutes les applications qui se trouvent actuellement dans le modèle.
- N'affectez pas un modèle d'application ThinApp à un poste de travail ou à un pool si le modèle contient une application ThinApp qui est déjà affectée à ce poste de travail ou à ce pool. De plus, n'affectez pas un modèle d'application ThinApp au même poste de travail ou pool plusieurs fois avec un type d'installation différent. View Administrator renverra des erreurs d'affectation ThinApp dans ces deux situations.
- Bien que l'affectation d'applications ThinApp à des postes de travail locaux ne soit pas prise en charge, View Administrator ne vous empêche pas d'effectuer l'opération. Pour tester l'affectation d'applications ThinApp à des postes de travail locaux, vous devez satisfaire certaines exigences. Si vous prévoyez de diffuser une application ThinApp, vérifiez que View Agent dans le poste de travail en mode local peut accéder au partage de réseau qui héberge le référentiel ThinApp. Les applications ThinApp continues fonctionnent uniquement lorsque le système client est connecté au réseau.

  L'affectation d'applications ThinApp et leur suppression d'un poste de travail fonctionnent uniquement si View Connection Server et View Agent dans le poste de travail en mode local peuvent accéder au partage de réseau qui héberge le référentiel ThinApp.

AVERTISSEMENT La restauration d'un poste de travail peut entraîner l'acquisition par Connection Server d'informations erronées sur les applications ThinApp sur le poste de travail restauré.

Affecter une application ThinApp à plusieurs postes de travail

Vous pouvez affecter une application ThinApp particulière à un ou plusieurs postes de travail.

Prérequis

Analysez un référentiel d'applications et ajoutez des applications ThinApp sélectionnées à View Administrator. Reportez-vous à la section « Ajouter des applications ThinApp à View Administrator », page 330.

Procédure

1 Sélectionnez **[Inventory (Inventaire)] > [ThinApps (Applications ThinApp)]** et sélectionnez l'application ThinApp.

2 Dans le menu déroulant **[Add Assignment (Ajouter une affectation)]** , sélectionnez **[Desktops (Postes de travail)]** .

Les postes de travail auxquels l'application ThinApp n'est pas déjà affectée apparaissent dans le tableau.

Option	Action
Find a specific desktop (Rechercher un poste de travail spécifique)	Saisissez le nom du poste de travail dans la zone de texte **[Find (Rechercher)]** et cliquez sur **[Find (Rechercher)]** .
Find all of the desktops that follow the same naming convention (Rechercher tous les postes de travail qui suivent la même convention de dénomination)	Saisissez un nom partiel de poste de travail dans la zone de texte **[Find (Rechercher)]** et cliquez sur **[Find (Rechercher)]** .

3 Sélectionnez les postes de travail auxquels vous voulez affecter l'application ThinApp et cliquez sur **[Add (Ajouter)]** .

Vous pouvez appuyer sur Ctrl+clic ou Maj+clic pour sélectionner plusieurs postes de travail.

4 Sélectionnez un type d'installation et cliquez sur **[OK]** .

Option	Action
Streaming (En continu)	Installe un raccourci vers l'application sur le poste de travail. Le raccourci pointe vers l'application sur le partage de réseau qui héberge le référentiel. Les utilisateurs doivent avoir accès au partage de réseau pour exécuter l'application.
Full (Complète)	Installe l'application complète sur le système de fichiers local.

Certaines applications ThinApp ne prennent pas en charge ces deux types d'installation. La façon dont le package d'applications a été créé détermine les types d'installation disponibles.

View Administrator commence à installer l'application ThinApp quelques minutes plus tard. Quand l'installation est terminée, l'application est disponible pour tous les utilisateurs des postes de travail.

Affecter plusieurs applications ThinApp à un poste de travail

Vous pouvez affecter une ou plusieurs applications ThinApp à un poste de travail particulier.

Prérequis

Analysez un référentiel d'applications et ajoutez des applications ThinApp sélectionnées à View Administrator. Reportez-vous à la section « Ajouter des applications ThinApp à View Administrator », page 330.

Procédure

1 Sélectionnez **[Inventory (Inventaire)] > [Desktops (Postes de travail)]** et double-cliquez sur le nom du poste de travail dans la colonne Desktop (Poste de travail).

2 Sous l'onglet **[Summary (Résumé)]** , cliquez sur **[Add Assignment (Ajouter une affectation)]** dans le volet ThinApps (Applications ThinApp).

Les applications ThinApp qui ne sont pas déjà affectées au poste de travail apparaissent dans le tableau.

3 Pour rechercher une application particulière, saisissez le nom de l'application dans la zone de texte **[Find (Rechercher)]** et cliquez sur **[Find (Rechercher)]** .

4 Sélectionnez une application ThinApp à affecter au poste de travail et cliquez sur **[Add (Ajouter)]** .

Répétez cette étape pour ajouter plusieurs applications.

5 Sélectionnez un type d'installation et cliquez sur **[OK]** .

Option	Action
Streaming (En continu)	Installe un raccourci vers l'application sur le poste de travail. Le raccourci pointe vers l'application sur le partage de réseau qui héberge le référentiel. Les utilisateurs doivent avoir accès au partage de réseau pour exécuter l'application.
Full (Complète)	Installe l'application complète sur le système de fichiers local.

Certaines applications ThinApp ne prennent pas en charge ces deux types d'installation. La façon dont le package d'applications a été créé détermine les types d'installation disponibles.

View Administrator commence à installer les applications ThinApp quelques minutes plus tard. Quand l'installation est terminée, les applications sont disponibles pour tous les utilisateurs du poste de travail.

Affecter une application ThinApp à plusieurs pools

Vous pouvez affecter une application ThinApp particulière à un ou plusieurs pools.

Si vous affectez une application ThinApp à un pool de clone lié, puis que vous actualisez, recomposez ou rééquilibrez le pool, View Administrator réinstalle l'application pour vous. Vous n'avez pas à réinstaller manuellement l'application.

Prérequis

Analysez un référentiel d'applications et ajoutez des applications ThinApp sélectionnées à View Administrator. Reportez-vous à la section « Ajouter des applications ThinApp à View Administrator », page 330.

Procédure

1 Sélectionnez **[Inventory (Inventaire)]** > **[ThinApps (Applications ThinApp)]** et sélectionnez l'application ThinApp.

2 Dans le menu déroulant **[Add Assignment (Ajouter une affectation)]** , sélectionnez **[Pools]** .

Les pools auxquels l'application ThinApp n'est pas déjà affectée apparaissent dans le tableau.

Option	Action
Find a specific pool (Rechercher un pool spécifique)	Saisissez le nom du pool dans la zone de texte **[Find (Rechercher)]** et cliquez sur **[Find (Rechercher)]** .
Find all of the pools that follow the same naming convention (Rechercher tous les pools qui suivent la même convention de dénomination)	Saisissez un nom partiel de pool dans la zone de texte **[Find (Rechercher)]** et cliquez sur **[Find (Rechercher)]** .

3 Sélectionnez les pools auxquels vous voulez affecter l'application ThinApp et cliquez sur **[Add (Ajouter)]** .

Vous pouvez appuyer sur Ctrl+clic ou Maj+clic pour sélectionner plusieurs pools.

4 Sélectionnez un type d'installation et cliquez sur **[OK]** .

Option	Action
Streaming (En continu)	Installe un raccourci vers l'application sur le poste de travail. Le raccourci pointe vers l'application sur le partage de réseau qui héberge le référentiel. Les utilisateurs doivent avoir accès au partage de réseau pour exécuter l'application.
Full (Complète)	Installe l'application complète sur le système de fichiers local.

Certaines applications ThinApp ne prennent pas en charge ces deux types d'installation. La façon dont le package d'applications a été créé détermine les types d'installation disponibles.

View Administrator commence à installer l'application ThinApp lors de la première ouverture de session de l'utilisateur sur un poste de travail dans le pool. Quand l'installation est terminée, l'application est disponible pour tous les utilisateurs du poste de travail.

Affecter plusieurs applications ThinApp à un pool

Vous pouvez affecter une ou plusieurs applications ThinApp à un pool particulier.

Si vous affectez une application ThinApp à un pool de clone lié, puis que vous actualisez, recomposez ou rééquilibrez le pool, View Administrator réinstalle l'application pour vous. Vous n'avez pas à réinstaller manuellement l'application.

Prérequis

Analysez un référentiel d'applications et ajoutez des applications ThinApp sélectionnées à View Administrator. Reportez-vous à la section « Ajouter des applications ThinApp à View Administrator », page 330.

Procédure

1 Sélectionnez **[Inventory (Inventaire)]** > **[Pools]** et double-cliquez sur l'ID de pool.

2 Sous l'onglet **[Inventory (Inventaire)]** , cliquez sur **[ThinApps (Applications ThinApp)]** et cliquez sur **[Add Assignment (Ajouter une affectation)]** .

Les applications ThinApp qui ne sont pas déjà affectées au pool apparaissent dans le tableau.

3 Pour rechercher une application particulière, saisissez le nom de l'application ThinApp dans la zone de texte **[Find (Rechercher)]** et cliquez sur **[Find (Rechercher)]** .

4 Sélectionnez une application ThinApp à affecter au pool et cliquez sur **[Add (Ajouter)]** .

Répétez cette étape pour sélectionner plusieurs applications.

5 Sélectionnez un type d'installation et cliquez sur **[OK]** .

Option	Action
Streaming (En continu)	Installe un raccourci vers l'application sur le poste de travail. Le raccourci pointe vers l'application sur le partage de réseau qui héberge le référentiel. Les utilisateurs doivent avoir accès au partage de réseau pour exécuter l'application.
Full (Complète)	Installe l'application complète sur le système de fichiers local.

Certaines applications ThinApp ne prennent pas en charge ces deux types d'installation. La façon dont le package d'applications a été créé détermine les types d'installation disponibles.

View Administrator commence à installer les applications ThinApp lors de la première ouverture de session de l'utilisateur sur un poste de travail dans le pool. Quand l'installation est terminée, les applications sont disponibles pour tous les utilisateurs du poste de travail.

Affecter un modèle d'application ThinApp à un poste de travail ou à un pool

Vous pouvez rationaliser la distribution de plusieurs applications ThinApp en affectant un modèle d'application ThinApp à un poste de travail ou à un pool.

Lorsque vous affectez un modèle d'application ThinApp à un poste de travail ou à un pool, View Administrator installe les applications ThinApp qui se trouvent actuellement dans le modèle.

Prérequis

Créez un modèle d'application ThinApp. Reportez-vous à la section « Créer un modèle d'application ThinApp », page 331.

Procédure

1 Dans View Administrator, sélectionnez **[Inventory (Inventaire)]** > **[ThinApps (Applications ThinApp)]** .

2 Sélectionnez le modèle d'application ThinApp.

3 Dans le menu déroulant **[Add Assignment (Ajouter une affectation)]** , sélectionnez **[Desktops (Postes de travail)]** ou **[Pools]** .

Tous les postes de travail ou pools apparaissent dans le tableau.

Option	Action
Find a specific desktop or pool (Rechercher un poste de travail ou un pool spécifique)	Saisissez le nom du poste de travail ou du pool dans la zone de texte **[Find (Rechercher)]** et cliquez sur **[Find (Rechercher)]** .
Find all of the desktops or pools that follow the same naming convention (Rechercher tous les postes de travail ou pools qui suivent la même convention de dénomination)	Saisissez un nom partiel de poste de travail ou de pool dans la zone de texte **[Find (Rechercher)]** et cliquez sur **[Find (Rechercher)]** .

4 Sélectionnez les postes de travail ou les pools auxquels vous voulez affecter le modèle d'application ThinApp et cliquez sur **[Add (Ajouter)]** .

Répétez cette étape pour sélectionner plusieurs postes de travail ou pools.

5 Sélectionnez un type d'installation et cliquez sur **[OK]** .

Option	Action
Streaming (En continu)	Installe un raccourci vers l'application sur le poste de travail. Le raccourci pointe vers l'application sur le partage de réseau qui héberge le référentiel. Les utilisateurs doivent avoir accès au partage de réseau pour exécuter l'application.
Full (Complète)	Installe l'application complète sur le système de fichiers local.

Certaines applications ThinApp ne prennent pas en charge ces deux types d'installation. La façon dont le package d'applications a été créé détermine les types d'installation disponibles.

Lorsque vous affectez un modèle d'application ThinApp à un poste de travail, View Administrator commence à installer les applications dans le modèle quelques minutes plus tard. Lorsque vous affectez un modèle d'application ThinApp à un pool, View Administrator commence à installer les applications dans le modèle la première fois qu'un utilisateur ouvre une session sur un poste de travail dans le pool. Quand l'installation est terminée, les applications sont disponibles pour tous les utilisateurs du poste de travail ou du pool.

View Administrator renvoie une erreur d'affectation d'application si un modèle d'application ThinApp contient une application déjà affectée au poste de travail ou au pool.

Consulter des affectations d'application ThinApp

Vous pouvez consulter tous les postes de travail et pools auxquels une application ThinApp particulière est actuellement affectée. Vous pouvez également consulter toutes les applications ThinApp affectées à un poste de travail ou un pool particulier.

Prérequis

Familiarisez-vous avec les valeurs d'état d'installation d'application ThinApp dans la section « Valeurs d'état d'installation d'application ThinApp », page 338.

Procédure

- Sélectionnez les affectations d'application ThinApp que vous voulez consulter.

Option	Action
Review all of the desktops and pools that a particular ThinApp application is assigned to (Consulter tous les postes de travail et pools auxquels une application ThinApp particulière est affectée)	Sélectionnez **[Inventory (Inventaire)] > [ThinApps (Applications ThinApp)]** et double-cliquez sur le nom de l'application ThinApp. L'onglet **[Assignments (Affectations)]** montre les postes de travail et les pools auxquels l'application est actuellement affectée, y compris le type d'installation. L'onglet **[Desktops (Postes de travail)]** montre les postes de travail qui sont actuellement associés à l'application, y compris les informations d'état d'installation. REMARQUE Lorsque vous affectez une application ThinApp à un pool, des postes de travail dans le pool apparaissent sous l'onglet **[Desktops (Postes de travail)]** uniquement après l'installation de l'application.
Review all of the ThinApp applications that are assigned to a particular desktop (Consulter toutes les applications ThinApp qui sont affectées à un poste de travail particulier)	Sélectionnez **[Inventory (Inventaire)] > [Desktops (Postes de travail)]** et double-cliquez sur le nom du poste de travail dans la colonne Desktop (Poste de travail). Le volet ThinApps (Applications ThinApp) sous l'onglet **[Summary (Résumé)]** montre chaque application qui est actuellement affectée au poste de travail, y compris l'état d'installation.
Review all of the ThinApp applications that are assigned to a particular pool (Consulter toutes les applications ThinApp qui sont affectées à un pool particulier)	Sélectionnez **[Inventory (Inventaire)] > [Pools]** , double-cliquez sur l'ID de pool, sélectionnez l'onglet **[Inventory (Inventaire)]** et cliquez sur **[ThinApps (Applications ThinApp)]** . Le volet ThinApp Assignments (Affectations ThinApp) montre chaque application actuellement affectée au pool.

Valeurs d'état d'installation d'application ThinApp

Après avoir affecté une application ThinApp à un poste de travail ou à un pool, View Administrator indique l'état de l'installation.

Tableau 13-1 décrit chaque valeur d'état.

Tableau 13-1. État de l'installation d'une application ThinApp

État	Description
Assigned (Affecté)	L'application ThinApp est affectée au poste de travail.
Install Error (Erreur d'installation)	Une erreur s'est produite lorsque View Administrator a tenté d'installer l'application ThinApp.
Uninstall Error (Erreur de désinstallation)	Une erreur s'est produite lorsque View Administrator a tenté de désinstaller l'application ThinApp.
Installed (Installé)	L'application ThinApp est installée.

Tableau 13-1. État de l'installation d'une application ThinApp (suite)

État	Description
Pending Install (Installation en attente)	View Administrator tente d'installer l'application ThinApp. Vous ne pouvez pas supprimer l'affectation d'une application dans cet état. **Remarque** Cette valeur n'apparaît pas pour les postes de travail dans des pools.
Pending Uninstall (Désinstallation en attente)	View Administrator tente de désinstaller l'application ThinApp.

Afficher des informations de package MSI

Après avoir ajouté une application ThinApp à View Administrator, vous pouvez afficher des informations sur son package MSI.

Procédure

1 Dans View Administrator, sélectionnez **[Inventory (Inventaire)] > [ThinApps (Applications ThinApp)]** .

L'onglet **[Summary (Résumé)]** répertorie les applications actuellement disponibles et montre le nombre d'affectations complètes et en continu.

2 Double-cliquez sur le nom de l'application dans la colonne ThinApp.

3 Sélectionnez l'onglet **[Summary (Résumé)]** pour voir des informations générales sur le package MSI.

4 Cliquez sur **[Package Info (Infos sur le package)]** pour voir des informations détaillées sur le package MSI.

Maintenance d'applications ThinApp dans View Administrator

La maintenance d'applications ThinApp dans View Administrator implique des tâches telles que la suppression d'affectations d'applications ThinApp, la suppression d'applications ThinApp et de référentiels d'applications, ainsi que la modification et la suppression de modèles d'application ThinApp.

Remarque Pour mettre à niveau une application ThinApp, vous devez supprimer l'affectation et supprimer la version antérieure de l'application, puis ajouter et affecter la nouvelle version.

- Supprimer une affectation d'application ThinApp de plusieurs postes de travail page 340

  Vous pouvez supprimer une affectation d'une application ThinApp particulière d'un ou plusieurs postes de travail.

- Supprimer plusieurs affectations d'application ThinApp d'un poste de travail page 340

  Vous pouvez supprimer des affectations d'une ou plusieurs applications ThinApp d'un poste de travail particulier.

- Supprimer une affectation d'application ThinApp de plusieurs pools page 341

  Vous pouvez supprimer une affectation d'une application ThinApp particulière d'un ou plusieurs pools.

- Supprimer plusieurs affectations d'application ThinApp d'un pool page 341

  Vous pouvez supprimer une ou plusieurs affectations d'application ThinApp d'un pool particulier.

- Supprimer une application ThinApp de View Administrator page 341

  Lorsque vous supprimez une application ThinApp de View Administrator, vous ne pouvez plus affecter l'application à des postes de travail et des pools.

- Modifier ou supprimer un modèle d'application ThinApp page 342

  Vous pouvez ajouter et supprimer des applications d'un modèle d'application ThinApp. Vous pouvez également supprimer un modèle d'application ThinApp.

- Supprimer un référentiel d'applications page 342

  Vous pouvez supprimer un référentiel d'applications de View Administrator.

Supprimer une affectation d'application ThinApp de plusieurs postes de travail

Vous pouvez supprimer une affectation d'une application ThinApp particulière d'un ou plusieurs postes de travail.

Prérequis

Informez les utilisateurs des postes de travail que vous prévoyez de supprimer l'application.

Procédure

1. Sélectionnez **[Inventory (Inventaire)] > [ThinApps (Applications ThinApp)]** et double-cliquez sur le nom de l'application ThinApp.
2. Sous l'onglet **[Assignments (Affectations)]** , sélectionnez un poste de travail et cliquez sur **[Remove Assignment (Supprimer une affectation)]** .

   Vous pouvez appuyer sur Ctrl+clic ou Maj+clic pour sélectionner plusieurs postes de travail.

View Administrator désinstalle l'application ThinApp quelques minutes plus tard.

IMPORTANT Si un utilisateur final utilise l'application ThinApp au moment où View Administrator tente de désinstaller l'application, la désinstallation échoue et l'état de l'application passe sur Uninstall Error (Erreur de désinstallation). Lorsque cette erreur se produit, vous devez d'abord désinstaller manuellement les fichiers de l'application ThinApp depuis le poste de travail View puis cliquer sur **[Force Clear Assignment (Forcer l'effacement d'affectation)]** dans View Administrator.

Supprimer plusieurs affectations d'application ThinApp d'un poste de travail

Vous pouvez supprimer des affectations d'une ou plusieurs applications ThinApp d'un poste de travail particulier.

Prérequis

Informez les utilisateurs du poste de travail que vous prévoyez de supprimer les applications.

Procédure

1. Sélectionnez **[Inventory (Inventaire)] > [Desktops (Postes de travail)]** et double-cliquez sur le nom du poste de travail dans la colonne Desktop (Poste de travail).
2. Sous l'onglet **[Summary (Résumé)]** , sélectionnez l'application ThinApp et cliquez sur **[Remove Assignment (Supprimer une affectation)]** dans le volet ThinApps (Applications ThinApp).

   Répétez cette étape pour supprimer une autre affectation d'application.

View Administrator désinstalle l'application ThinApp quelques minutes plus tard.

IMPORTANT Si un utilisateur final utilise l'application ThinApp au moment où View Administrator tente de désinstaller l'application, la désinstallation échoue et l'état de l'application passe sur Uninstall Error (Erreur de désinstallation). Lorsque cette erreur se produit, vous devez d'abord désinstaller manuellement les fichiers de l'application ThinApp depuis le poste de travail View puis cliquer sur **[Force Clear Assignment (Forcer l'effacement d'affectation)]** dans View Administrator.

Supprimer une affectation d'application ThinApp de plusieurs pools

Vous pouvez supprimer une affectation d'une application ThinApp particulière d'un ou plusieurs pools.

Prérequis

Informez les utilisateurs des postes de travail dans les pools que vous prévoyez de supprimer l'application.

Procédure

1 Sélectionnez **[Inventory (Inventaire)] > [ThinApps (Applications ThinApp)]** et double-cliquez sur le nom de l'application ThinApp.

2 Sous l'onglet **[Assignments (Affectations)]** , sélectionnez un pool et cliquez sur **[Remove Assignment (Supprimer une affectation)]** .

Vous pouvez appuyer sur Ctrl+clic ou Maj+clic pour sélectionner plusieurs pools.

View Administrator désinstalle l'application ThinApp lors de la première ouverture de session de l'utilisateur sur un poste de travail dans le pool.

Supprimer plusieurs affectations d'application ThinApp d'un pool

Vous pouvez supprimer une ou plusieurs affectations d'application ThinApp d'un pool particulier.

Prérequis

Informez les utilisateurs des postes de travail dans le pool que vous prévoyez de supprimer les applications.

Procédure

1 Sélectionnez **[Inventory (Inventaire)] > [Pools]** et double-cliquez sur l'ID de pool.

2 Sous l'onglet **[Inventory (Inventaire)]** , cliquez sur **[ThinApps (Applications ThinApp)]** , sélectionnez l'application ThinApp et cliquez sur **[Remove Assignment (Supprimer une affectation)]** .

Répétez cette étape pour supprimer plusieurs applications.

View Administrator désinstalle les applications ThinApp lors de la première ouverture de session de l'utilisateur sur un poste de travail dans le pool.

Supprimer une application ThinApp de View Administrator

Lorsque vous supprimez une application ThinApp de View Administrator, vous ne pouvez plus affecter l'application à des postes de travail et des pools.

Vous devrez peut-être supprimer une application ThinApp si votre entreprise décide de la remplacer par l'application d'un fournisseur différent.

Remarque Vous ne pouvez pas supprimer une application ThinApp si elle est déjà affectée à un poste de travail ou à un pool ou si elle est dans l'état Pending Uninstall (Désinstallation en attente).

Prérequis

Si une application ThinApp est actuellement affectée à un poste de travail ou un pool, supprimez l'affectation du poste de travail ou du pool.

Procédure

1 Dans View Administrator, sélectionnez **[Inventory (Inventaire)] > [ThinApps (Applications ThinApp)]** et sélectionnez l'application ThinApp.

2 Cliquez sur **[Remove ThinApp (Supprimer l'application ThinApp)]** .

3 Cliquez sur **[OK]** .

Modifier ou supprimer un modèle d'application ThinApp

Vous pouvez ajouter et supprimer des applications d'un modèle d'application ThinApp. Vous pouvez également supprimer un modèle d'application ThinApp.

Si vous ajoutez une application à un modèle d'application ThinApp après avoir affecté un modèle à un poste de travail ou à un pool, View Administrator n'affecte pas automatiquement la nouvelle application au poste de travail ou au pool. Si vous supprimez une application d'un modèle d'application ThinApp qui était précédemment affecté à un poste de travail ou à un pool, l'application reste affectée au poste de travail ou au pool.

Procédure

- Dans View Administrator, sélectionnez **[Inventory (Inventaire)] > [ThinApps (Applications ThinApp)]** et sélectionnez le modèle d'application ThinApp.

Option	Action
Add or remove ThinApp applications from the template (Ajouter ou supprimer des applications ThinApp du modèle)	Cliquez sur **[Edit Template (Modifier le modèle)]** .
Delete the template (Supprimer le modèle)	Cliquez sur **[Delete Template (Supprimer le modèle)]** .

Supprimer un référentiel d'applications

Vous pouvez supprimer un référentiel d'applications de View Administrator.

Vous devrez peut-être supprimer un référentiel d'applications si vous n'avez plus besoin des packages MSI qu'il contient, ou si vous avez besoin de déplacer les packages MSI vers un partage de réseau différent. Vous ne pouvez pas modifier le chemin de partage d'un référentiel d'applications dans View Administrator.

Procédure

1 Dans View Administrator, sélectionnez **[View Configuration (Configuration de View)] > [ThinApp Configuration (Configuration d'application ThinApp)]** et sélectionnez le référentiel d'applications.

2 Cliquez sur **[Remove Repository (Supprimer le référentiel)]** .

Contrôle et dépannage d'applications ThinApp dans View Administrator

View Administrator journalise des événements liés à la gestion d'applications ThinApp dans la base de données Events and Reporting (Événements et reporting). Vous pouvez voir ces événements sous l'onglet **[Events (Événements)]** dans View Administrator.

Un événement apparaît sous l'onglet **[Events (Événements)]** lorsque les situations suivantes se produisent.

- Une application ThinApp est affectée ou une affectation d'application est supprimée.
- Une application ThinApp est installée ou désinstallée sur un poste de travail.
- Une application ThinApp ne peut pas être installée ou désinstallée.
- Un référentiel d'applications ThinApp est enregistré, modifié ou supprimé de View Administrator.

- Une application ThinApp est ajoutée sur View Administrator.

Des conseils de dépannage sont disponibles pour des problèmes de gestion d'applications ThinApp communs.

Impossible d'enregistrer un référentiel d'applications

Vous ne pouvez pas enregistrer un référentiel d'applications dans View Administrator.

Problème

Vous recevez un message d'erreur lorsque vous tentez d'enregistrer un référentiel d'applications dans View Administrator.

Cause

L'hôte de View Connection Server ne peut pas accéder au partage de réseau qui héberge le référentiel d'applications. Le chemin du partage de réseau que vous avez saisi dans la zone de texte **[Share path (Chemin de partage)]** est peut-être incorrect, le partage de réseau qui héberge le référentiel d'applications se trouve dans un domaine qui n'est pas accessible depuis l'hôte de View Connection Server ou les autorisations de partage de réseau n'ont pas été configurées correctement.

Solution

- Si le chemin de partage de réseau est incorrect, saisissez le chemin de partage de réseau correct. Les chemins de partage de réseau qui contiennent des adresses IP ne sont pas pris en charge.
- Si le partage de réseau ne se trouve pas dans un domaine accessible, copiez vos packages d'applications dans un partage de réseau dans un domaine qui est accessible depuis l'hôte de View Connection Server.
- Vérifiez que les autorisations de fichier et de partage sur le dossier partagé donnent un accès en lecture aux ordinateurs de domaine du groupe Active Directory intégré. Si vous prévoyez d'affecter des applications ThinApp à des contrôleurs de domaine, vérifiez que les autorisations de fichier et de partage donnent également un accès en lecture aux contrôleurs de domaine du groupe Active Directory intégré. Après avoir configuré ou modifié des autorisations, cela peut prendre jusqu'à 20 minutes pour que le partage de réseau devienne accessible.

Impossible d'ajouter des applications ThinApp à View Administrator

View Administrator ne peut pas ajouter d'applications ThinApp à View Administrator.

Problème

Aucun package MSI n'est disponible lorsque vous cliquez sur **[Scan New ThinApps (Analyser de nouvelles applications ThinApp)]** dans View Administrator.

Cause

Les packages d'applications ne sont pas au format MSI ou l'hôte de View Connection Server ne peut pas accéder aux répertoires dans le partage de réseau.

Solution

- Vérifiez que les packages d'applications dans le référentiel d'applications sont au format MSI.
- Vérifiez que le partage réseau satisfait les exigences View pour les applications ThinApp. Reportez-vous à la section « Configuration requise de View pour des applications ThinApp », page 327 pour plus d'informations.
- Vérifiez que les répertoires dans le partage de réseau ont les autorisations correctes. Reportez-vous à la section « Impossible d'enregistrer un référentiel d'applications », page 343 pour plus d'informations.

Des messages apparaissent dans le fichier journal de débogage de View Connection Server lorsqu'un référentiel d'applications est analysé. Les fichiers journaux de View Connection Server sont situés sur l'hôte de View Connection Server dans le répertoire *drive*:\Documents and Settings\All Users\Application Data\VMware\VDM\logs.

Impossible d'affecter un modèle d'application ThinApp

Vous ne pouvez pas affecter un modèle d'application ThinApp à un poste de travail ou à un pool.

Problème

View Administrator renvoie une erreur d'affectation lorsque vous tentez d'affecter un modèle d'application ThinApp à un poste de travail ou à un pool.

Cause

Le modèle d'application ThinApp contient une application qui est déjà affectée au poste de travail ou au pool, ou le modèle d'application ThinApp était déjà affecté au poste de travail ou au pool avec un type d'installation différent.

Solution

Si le modèle contient une application ThinApp qui est déjà affectée au poste de travail ou au pool, créez un nouveau modèle qui ne contient pas l'application ou modifiez le modèle existant et supprimez l'application. Affectez le nouveau modèle ou le modèle modifié au poste de travail ou au pool.

Pour modifier le type d'installation d'une application ThinApp, vous devez supprimer l'affectation d'application existante du poste de travail ou du pool. Quand l'application ThinApp est désinstallée, vous pouvez l'affecter au poste de travail ou au pool avec un type d'installation différent.

L'application ThinApp n'est pas installée

View Administrator ne peut pas installer une application ThinApp.

Problème

L'état d'installation d'application ThinApp indique Pending Install (Installation en attente) ou Install Error (Erreur d'installation).

Cause

Certaines des causes communes de ce problème sont les suivantes :

- L'espace disque sur le poste de travail était insuffisant pour installer l'application ThinApp.
- La connectivité réseau a été perdue entre l'hôte de View Connection Server et le poste de travail ou entre l'hôte de View Connection Server et le référentiel d'applications.
- L'application ThinApp n'était pas accessible dans le partage de réseau.
- L'application ThinApp a été installée précédemment ou le répertoire ou le fichier existe déjà sur le poste de travail.

Pour plus d'informations sur la cause du problème, vous pouvez consulter les fichiers journaux de View Agent et de View Connection Server.

Les fichiers journaux de View Agent sont situés sur le poste de travail dans *drive*:\Documents and Settings\All Users\Application Data\VMware\VDM\logs pour les système Windows XP et dans *drive*:\ProgramData\VMware\VDM\logs pour les systèmes Windows 7.

Les fichiers journaux de View Connection Server sont situés sur l'hôte de View Connection Server dans le répertoire *drive*:\Documents and Settings\All Users\Application Data\VMware\VDM\logs.

Solution

1 Dans View Administrator, sélectionnez **[Inventory (Inventaire)] > [ThinApps (Applications ThinApp)]** .

2 Cliquez sur le nom de l'application ThinApp.

3 Sous l'onglet **[Desktops (Postes de travail)]** , sélectionnez le poste de travail et cliquez sur **[Retry Install (Réessayer l'installation)]** pour réinstaller l'application ThinApp.

L'application ThinApp n'est pas désinstallée

View Administrator ne peut pas désinstaller une application ThinApp.

Problème

L'état d'installation de l'application ThinApp affiche Uninstall Error (Erreur de désinstallation).

Cause

Certaines des causes communes à cette erreur sont les suivantes :

- L'application ThinApp était occupée quand View Administrator tentait de la désinstaller.
- La connectivité réseau a été perdue entre l'hôte de View Connection Server et le poste de travail.

Pour plus d'informations sur la cause du problème, vous pouvez consulter les fichiers journaux de View Agent et de View Connection Server.

Les fichiers journaux de View Agent sont situés sur le poste de travail dans *drive*:\Documents and Settings\All Users\Application Data\VMware\VDM\logs pour les système Windows XP et dans *drive*:\ProgramData\VMware\VDM\logs pour les systèmes Windows 7.

Les fichiers journaux de View Connection Server sont situés sur l'hôte de View Connection Server dans le répertoire *drive*:\Documents and Settings\All Users\Application Data\VMware\VDM\logs.

Solution

1 Dans View Administrator, sélectionnez **[Inventory (Inventaire)] > [ThinApps (Applications ThinApp)]** .

2 Cliquez sur le nom de l'application ThinApp.

3 Cliquez sur l'onglet **[Desktops (Postes de travail)]** , sélectionnez le poste de travail et cliquez sur **[Retry Uninstall (Réessayer la désinstallation)]** pour tenter de nouveau l'opération de désinstallation.

4 Si l'opération de désinstallation échoue toujours, supprimez manuellement l'application ThinApp du poste de travail et cliquez sur **[Force Clear Assignment (Forcer l'effacement d'affectation)]** .

   Cette commande efface l'affectation d'application ThinApp dans View Administrator. Elle ne supprime aucun fichier ou paramètre dans le poste de travail.

   IMPORTANT N'utilisez cette commande qu'après avoir supprimé manuellement l'application ThinApp du poste de travail.

Le package MSI est non valide

View Administrator signale un package MSI non valide dans un référentiel d'applications.

Problème

View Administrator signale qu'un package MSI est non valide au cours d'une opération d'analyse.

Cause

Certaines des causes communes de ce problème sont les suivantes :

- Le fichier MSI est corrompu.
- Le fichier MSI n'a pas été créé avec ThinApp.
- Le fichier MSI a été créé ou reconditionné avec une version non prise en charge de ThinApp. Vous devez utiliser ThinApp version 4.6 ou supérieure.

Solution

Pour plus d'informations sur la résolution des problèmes avec des packages MSI, consultez le guide *ThinApp User's Guide (Guide de l'utilisateur de ThinApp)*.

Exemple de configuration d'application ThinApp

L'exemple de configuration d'application ThinApp vous guide pas à pas dans une configuration d'application ThinApp typique, en commençant par la capture et l'assemblage d'applications et en terminant par la vérification de l'état d'une installation.

Prérequis

Pour plus d'informations sur l'exécution des étapes dans cet exemple, reportez-vous aux rubriques suivantes :

- « Capture et stockage de packages d'applications », page 328
- « Affectation d'applications ThinApp à des postes de travail et des pools », page 332

Procédure

1 Téléchargez le logiciel ThinApp sur le site http://www.vmware.com/fr/products/thinapp et installez-le sur un ordinateur sain.

   View prend en charge ThinApp version 4.6 et supérieure.

2 Utilisez l'assistant ThinApp Setup Capture pour capturer et assembler vos applications au format MSI.

3 Créez un dossier partagé sur un ordinateur dans un domaine Active Directory accessible à votre hôte de View Connection Server et à vos postes de travail View et configurez les autorisations de fichier et de partage sur le dossier partagé pour donner un accès en lecture aux ordinateurs de domaine du groupe Active Directory intégré.

   Si vous prévoyez d'affecter des applications ThinApp à des contrôleurs de domaine, donnez également un accès en lecture aux contrôleurs de domaine du groupe Active Directory intégré.

4 Copiez vos packages MSI dans le dossier partagé.

5 Enregistrez le dossier partagé en tant que référentiel d'applications dans View Administrator.

6 Dans View Administrator, analysez les packages MSI dans le référentiel d'applications et ajoutez les applications ThinApp sélectionnées à View Administrator.

7 Décidez d'affecter les applications ThinApp à des postes de travail ou des pools.

   Si vous utilisez une convention de dénomination commune pour vos postes de travail, vous pouvez utiliser des affectations de postes de travail pour distribuer rapidement des applications à tous les postes de travail qui utilisent cette convention de dénomination. Si vous organisez vos pools par service ou par type d'utilisateur, vous pouvez utiliser des affectations de pools pour distribuer rapidement des applications à des services ou des utilisateurs spécifiques.

8 Dans View Administrator, sélectionnez les applications ThinApp à affecter à vos postes de travail ou à vos pools et spécifiez la méthode d'installation.

Option	Action
Streaming (En continu)	Installe un raccourci vers l'application sur le poste de travail. Le raccourci pointe vers l'application sur le partage de réseau qui héberge le référentiel. Les utilisateurs doivent avoir accès au partage de réseau pour exécuter l'application.
Full (Complète)	Installe l'application complète sur le système de fichiers local.

9 Dans View Administrator, vérifiez l'état d'installation des applications ThinApp.

Gestion de postes de travail locaux 14

Pour gérer des postes de travail utilisés en mode local, vous devez configurer l'environnement pour que les données soient transférées lorsque des utilisateurs empruntent des postes de travail View sur leurs systèmes locaux. Vous devez également gérer d'autres tâches lorsque des transferts de données ont lieu, telles que la restitution, la restauration et la sauvegarde de poste de travail, et définir des règles pour les actions que les utilisateurs peuvent initier.

Ce chapitre aborde les rubriques suivantes :

Avantages à utiliser des postes de travail View en mode local

Avec View Client with Local Mode, les utilisateurs peuvent emprunter et télécharger un poste de travail View sur un système local tel qu'un ordinateur portable. Les administrateurs peuvent gérer ces postes de travail View locaux en définissant des règles pour la fréquence des sauvegardes et des contacts avec le serveur, pour l'accès à des périphériques USB et pour l'autorisation de restitution des postes de travail.

Pour les employés dans des bureaux distants avec des connexions réseau de qualité médiocre, les applications peuvent s'exécuter plus rapidement sur un poste de travail View local que sur un poste de travail distant. De même, les utilisateurs peuvent utiliser la version locale du poste de travail avec ou sans connexion réseau.

Si une connexion réseau est présente sur le système client, le poste de travail emprunté continue de communiquer avec Serveur de connexion View afin de fournir des mises à jour de règles et d'assurer que les critères d'authentification mise en cache en local sont actualisés. Par défaut, le contact est entrepris toutes les 6 minutes.

Les postes de travail View en mode local se comportent de la même façon que les postes de travail distants équivalents qui peuvent déjà bénéficier de ressources locales. La latence est éliminée et les performances sont améliorées. Les utilisateurs peuvent se déconnecter de leur poste de travail View local puis de nouveau ouvrir une session sans se connecter au serveur Serveur de connexion View. Une fois l'accès au réseau restauré, ou lorsque l'utilisateur est prêt, la machine virtuelle empruntée peut être sauvegardée, restaurée ou restituée.

Utilisation de ressources locales

Une fois emprunté, un poste de travail local peut bénéficier des capacités de mémoire et de CPU du système local. Par exemple, la mémoire disponible au-delà de ce qui est requis pour les systèmes d'exploitation hôte et client est généralement divisée entre l'hôte et le poste de travail View local, quels que soient les paramètres de mémoire spécifiés pour la machine virtuelle dans vCenter Server. De la même façon, le poste de travail View local peut automatiquement utiliser jusqu'à deux CPU disponibles sur le système local, et vous pouvez configurer le poste de travail local pour utiliser jusqu'à quatre CPU.

Bien qu'un poste de travail local puisse bénéficier de ressources locales, un poste de travail View Windows 8, Windows 7 ou Windows Vista créé sur un hôte ESX/ESXi 3.5 ne peut pas produire d'effets 3D et Windows Aero. Cette limite s'applique même lorsque le poste de travail est emprunté pour une utilisation locale sur un hôte Windows 8, Windows 7 ou Windows Vista. Les effets Windows Aero et 3D ne sont disponibles que si le poste de travail View est créé à l'aide de vSphere 4.x ou supérieur.

Conservation de ressources de datacenter en nécessitant le mode local

Vous pouvez réduire les coûts de datacenter associés aux ressources de bande passante, de mémoire et de CPU en demandant que des postes de travail View soient téléchargés et utilisés uniquement en mode local. Cette stratégie est parfois appelée programme BRYO (bring-your-own-PC, apporter votre propre PC) pour les employés et les prestataires.

Emprunts

Lorsque le poste de travail View est emprunté, un snapshot est pris dans vCenter Server afin de préserver l'état de la machine virtuelle. La version vCenter Server du poste de travail est verrouillée pour qu'aucun autre utilisateur ne puisse y accéder. Lorsqu'un poste de travail View est verrouillé, les opérations de vCenter Server sont désactivées, y compris les opérations telles que la mise sous tension du poste de travail en ligne, la prise de snapshots et la modification des paramètres de la machine virtuelle. Toutefois, les administrateurs de View peuvent toujours surveiller la session locale et accéder à la version vCenter Server pour supprimer l'accès ou restaurer le poste de travail.

Sauvegardes

Lors des sauvegardes, un snapshot est pris sur le système client, pour conserver l'état de la machine virtuelle empruntée. Le différentiel entre ce snapshot et le snapshot dans vCenter Server est répliqué vers vCenter Server puis fusionné avec le snapshot qui s'y trouve. Le poste de travail View dans vCenter Server est mis à jour avec toutes les nouvelles données et configurations, mais le poste de travail local reste emprunté sur le système local et le verrou reste défini dans vCenter Server.

Restaurations Lors des restaurations, le poste de travail View local est ignoré et est déverrouillé dans vCenter Server. Les futures connexions client sont dirigées vers le poste de travail View dans vCenter Server jusqu'à ce que le poste de travail soit emprunté de nouveau.

Restitutions Lorsqu'un poste de travail View est restitué, un snapshot est pris sur le système client, afin de conserver l'état de la machine virtuelle. Le différentiel entre ce snapshot et le snapshot dans vCenter Server est répliqué vers vCenter Server puis fusionné avec le snapshot qui s'y trouve. La machine virtuelle dans vCenter Server est déverrouillée. Les futures connexions client sont dirigées vers le poste de travail View dans vCenter Server jusqu'à ce que le poste de travail soit emprunté de nouveau.

Les données sur chaque système local sont cryptées avec AES. Le chiffrement 128 bits est appliqué par défaut, mais vous pouvez configurer un chiffrement 192 ou 256 bits. Le poste de travail a une durée de vie contrôlée par une règle. Si le client perd le contact avec Serveur de connexion View, la durée maximale sans contact avec le serveur est la période au cours de laquelle l'utilisateur peut continuer à utiliser le poste de travail avant que son accès soit refusé. De même, si l'accès de l'utilisateur est supprimé, le système client devient inaccessible lorsque le cache expire ou que le client détecte cette modification via Serveur de connexion View.

View Client with Local Mode a les limites et restrictions suivantes :

- Vous devez disposer d'une licence Horizon View incluant le composant Local Mode.
- Les utilisateurs finaux ne peuvent pas accéder à leur poste de travail local au cours de restaurations et de restitutions.
- Cette fonction n'est disponible que pour les machines virtuelles gérées par vCenter Server.
- Vous ne pouvez pas utiliser View Persona Management avec des postes de travail exécutés en mode local.
- L'affectation de packages d'application créés avec VMware ThinApp n'est pas prise en charge pour les postes de travail View téléchargés et utilisés en mode local. La restauration d'un poste de travail peut entraîner l'acquisition par Serveur de connexion View d'informations erronées sur les applications ThinApp sur le poste de travail restauré.
- Pour des raisons de sécurité, vous ne pouvez pas accéder au CD-ROM hôte à partir du poste de travail View,
- ni copier et coller du texte ou des objets système tels que des fichiers et des dossiers entre le système local et le poste de travail View.

Présentation de la configuration d'un déploiement de poste de travail local

Pour créer et déployer des postes de travail View en mode local, vous devez posséder la licence requise, configurer un serveur Serveur de transfert View, utiliser une source de postes de travail gérée par vCenter Server et appliquer des paramètres et des règles spécifiques au mode local.

Lorsque vous créez des postes de travail pouvant être empruntés pour une utilisation sur des systèmes locaux d'utilisateurs finaux, en plus des tâches de configuration normales, vous devez effectuer plusieurs tâches pour le mode local.

1 Vérifiez que vous possédez une licence pour le composant VMware View with Local Mode.

  Dans View Administrator, allez dans **[Configuration de View] > [Licence produit et utilisation]** .

2 Vérifiez que le compte d'utilisateur utilisé pour accéder à vCenter Server depuis Serveur de connexion View dispose des privilèges d'administrateur requis.

Pour voir le compte d'utilisateur en cours d'utilisation, dans View Administrator, allez dans **[Configuration de View] > [Serveurs]** , sélectionnez le serveur vCenter Server et cliquez sur **[Modifier]** .

La liste de privilèges requis pour des opérations de vCenter Server est fournie dans le document *Installation de VMware Horizon View*, dans la section sur la configuration de comptes d'utilisateur pour vCenter Server.

3 Installez Serveur de transfert View dans une machine virtuelle et ajoutez ce serveur à une configuration de Serveur de connexion View.

Dans View Administrator, allez dans **[Configuration de View] > [Serveurs]** .

4 Si vous prévoyez d'utiliser des postes de travail de clone lié View Composer, configurez un référentiel de Serveur de transfert.

Dans View Administrator, allez dans **[Configuration de View] > [Serveurs] > [Serveurs de transfert] > [Référentiel du serveur de transfert]** .

5 Si vous prévoyez de créer un pool manuel, vérifiez que la source de postes de travail est une machine virtuelle gérée par vCenter Server.

6 Créez une machine virtuelle dans vCenter Server à utiliser comme source de postes de travail.

Si vous créez une machine virtuelle avec plus de mémoire virtuelle et de processeurs que n'en dispose un système client local, le poste de travail ne peut pas être emprunté et un message d'erreur apparaîtra.

7 Si vous prévoyez d'utiliser des postes de travail de clone lié, publiez l'image de base de View Composer des postes de travail en tant que package dans le référentiel de Serveur de transfert.

Vous pouvez publier l'image de base lorsque vous créez un pool ou après la création du pool.

8 Vérifiez que la règle **[Mode local]** est définie sur **[Autoriser]** pour le pool de postes de travail.

Dans View Administrator, allez dans l'onglet **[Règles]** pour ce pool.

9 Si vous voulez que les postes de travail s'exécutent en mode local uniquement pour que les utilisateurs aient toujours à emprunter le poste de travail, définissez la règle **[Mode distant]** sur **[Refuser]** .

Dans View Administrator, allez dans l'onglet **[Règles]** pour ce pool.

10 Demandez aux utilisateurs finaux d'installer View Client with Local Mode sur leurs systèmes locaux.

IMPORTANT Par ailleurs, prenez en compte les considérations suivantes lorsque vous prévoyez de déployer des postes de travail locaux :

- Lorsque vous créez un pool automatisé, utilisez une affectation dédiée et créez le pool uniquement pour les postes de travail prévus pour une utilisation en mode local. Les machines virtuelles conçues pour une utilisation en mode local peuvent être placées sur des magasins de données avec un IOPS inférieur au stockage prévu pour prendre en charge un nombre important de postes de travail View distants. De plus, comme l'affectation de packages ThinApp à des postes de travail locaux n'est pas prise en charge, il est recommandé d'affecter les packages ThinApp à des pools ne contenant pas de postes de travail locaux.
- En tant que meilleure pratique standard pour les postes de travail, assurez-vous qu'un mot de passe unique est créé pour le compte d'administrateur local sur chaque poste de travail View que vous prévoyez d'utiliser en mode local.
- Si vous configurez le poste de travail à utiliser l'authentification RSA, les utilisateurs finaux sont invités à fournir le jeton RSA lorsqu'ils ont une connexion réseau sur Serveur de connexion View mais ils n'y sont pas invités lorsqu'ils n'ont pas de connexion réseau.

Régler un poste de travail pour qu'il ne s'exécute qu'en mode local

Vous pouvez réduire les coûts de datacenter associés à la bande passante, à la mémoire et aux ressources de CPU en demandant que des postes de travail View soient téléchargés et utilisés uniquement en mode local.

Lorsqu'un poste de travail View est configuré pour s'exécuter uniquement en mode local, les utilisateurs finaux voient qu'un téléchargement et un emprunt sont requis lorsqu'ils sélectionnent le poste de travail dans View Client. Les options pour se connecter au poste de travail et pour le restituer ne sont pas disponibles pour les utilisateurs finaux.

Prérequis

- Vérifiez que le poste de travail View satisfait toutes les exigences pour être exécuté en mode local.

  Reportez-vous à la section « Présentation de la configuration d'un déploiement de poste de travail local », page 351.

- Familiarisez-vous avec les règles et les paramètres spécifiques au mode local.

  Reportez-vous à la section « Gestion des transferts de données », page 368.

Procédure

1 Dans View Administrator, voyez la règle pour le niveau approprié.

Option	Action
All desktops and pools (Tous les postes de travail et pools)	Sélectionnez **[Policies (Règles)]** > **[Global Policies (Règles générales)]** > **[View Policies (Règles de View)]** et cliquez sur **[Edit Policies (Modifier des règles)]** .
Single pool (Pool unique)	Sélectionnez **[Inventory (Inventaire)]** > **[Pools]** > **[*specific_pool*]** . Sous l'onglet **[Policies (Règles)]** , dans le volet **[View Policies (Règles de View)]** , cliquez sur **[Edit Policies (Modifier des règles)]** .
Single user (Utilisateur unique)	Sélectionnez **[Inventory (Inventaire)]** > **[Pools]** > **[*specific_pool*]** et sous l'onglet **[Policies (Règles)]** , cliquez sur **[User Overrides (Remplacements d'utilisateur)]** .

2 Définissez la règle de View **[Remote Mode (Mode distant)]** sur **[Deny (Refuser)]** .

Option	Action
All desktops and pools or a single pool (Tous les postes de travail et pools ou un pool unique)	Dans la boîte de dialogue Edit View Policies (Modifier des règles de View), définissez **[Remote Mode (Mode distant)]** sur **[Deny (Refuser)]** et cliquez sur **[OK]** .
Single user (Utilisateur unique)	Effectuez l'assistant Add User (Ajouter un utilisateur) pour spécifier l'utilisateur et définissez **[Remote Mode (Mode distant)]** sur **[Deny (Refuser)]** .

Le poste de travail requiert désormais un téléchargement et un emprunt.

Suivant

Si vous souhaitez empêcher les utilisateurs finaux de restituer de nouveau le poste de travail, définissez la règle **[User-initiated check in (Restitution initiée par l'utilisateur)]** sur **[Deny (Refuser)]** .

Si vous souhaitez empêcher les utilisateurs finaux de restaurer le poste de travail, définissez la règle **[User-initiated rollback (Restauration initiée par l'utilisateur)]** sur **[Deny (Refuser)]** .

Emprunt d'un poste de travail en mode local pour la première fois

La première fois qu'un utilisateur final emprunte un poste de travail View pour l'utiliser en mode local, le processus d'emprunt et de téléchargement implique plusieurs phases et prend plus de temps que pour des opérations d'emprunt qui se suivent.

Une fois qu'un utilisateur a ouvert une session avec View Client et qu'il obtient une liste d'un ou plusieurs postes de travail, il peut se connecter au poste de travail puis l'emprunter ou emprunter le poste de travail sans d'abord se connecter à distance.

IMPORTANT Vous ne pouvez pas emprunter un poste de travail si vous avez utilisé la fonction **[Log in as current user (Se connecter en tant qu'utilisateur actuel)]** lors de l'ouverture de session. Vous devez fermer View Client, le redémarrer, puis cocher la case **[Log in as current user (Se connecter en tant qu'utilisateur actuel)]** .

Si l'utilisateur final se connecte au poste de travail puis qu'il l'emprunte, sa session sur le poste de travail distant est fermée, la machine virtuelle dans le datacenter est verrouillée et une copie de la machine virtuelle est téléchargée pour l'utilisateur final.

Une fois le téléchargement terminé, la première fois que l'utilisateur final active le poste de travail local, des pilotes sont installés dans le poste de travail local. Les pilotes installés dépendent du système d'exploitation du poste de travail View et du matériel et du système d'exploitation de l'ordinateur local. Lors de l'installation des pilotes, les performances du poste de travail View sont affectées, en particulier si le poste de travail View exécute un système d'exploitation Windows XP.

Une fois les pilotes installés, l'utilisateur final est invité à redémarrer le poste de travail local.

REMARQUE Il arrive parfois que votre pointeur reste à l'intérieur de la fenêtre lorsque vous cliquez dans la fenêtre d'un poste de travail View au démarrage ou à l'arrêt du système d'exploitation client. Après le démarrage et l'exécution de VMware Tools, le pointeur est libéré. Si votre pointeur est capturé à l'intérieur de la fenêtre du poste de travail, vous pouvez le libérer en appuyant sur Ctrl+Alt.

La quantité de RAM et le nombre de CPU que le poste de travail View local utilise dépendent des capacités de l'ordinateur local. Le poste de travail View utilise NAT pour partager les adresses IP et MAC de l'ordinateur local. Pour plus d'informations, reportez-vous à la section « Configuration de l'utilisation d'une ressource de point de terminaison », page 378.

Meilleures pratiques pour le déploiement de postes de travail locaux

Les recommandations en termes de meilleures pratiques abordent les questions de mémoire, de puissance de traitement, ainsi que les divers composants affectant un déploiement du mode local.

Recommandations générales pour la plupart des déploiements

Configuration de machine virtuelle

Les postes de travail exécutés en mode local règlent automatiquement la quantité de mémoire et la puissance de traitement en fonction de la disponibilité sur l'ordinateur client. Grâce à cette fonctionnalité, vous pouvez configurer la quantité minimale de RAM et les CPU virtuelles requises par le système d'exploitation client lorsque vous créez la machine virtuelle dans vCenter Server.

Serveur de transfert View

Certaines fonctions de Serveur de transfert View sont gourmandes en CPU. Si vous prévoyez d'utiliser SSL pour des opérations en mode local, telles que l'emprunt et la restitution de postes de travail ou le réplication de données vers le datacenter, vous devez peut-être ajouter une CPU virtuelle à la machine virtuelle hébergeant Serveur de transfert. Vous aurez peut-être aussi besoin

d'une puissance de traitement accrue si vous activez la compression pour les opérations de réplication. Pour des exigences de mémoire et de processeur minimales, reportez-vous à la section du document *Installation de View* relative à la configuration requise pour Serveur de transfert View.

Pour déterminer le nombre d'instances de Serveur de transfert View à ajouter à Serveur de connexion View, vous devez décider si une disponibilité élevée est une considération importante. Auquel cas, ajoutez au moins deux instances. Si un Serveur de transfert tombe en panne, Serveur de connexion View envoie automatiquement des demandes à l'autre.

Lorsque vous calculez le nombre d'instances Serveur de transfert requises, tenez également compte du nombre d'utilisateurs finaux susceptibles de répliquer des données ou d'emprunter/restituer des postes de travail simultanément. Chaque instance Serveur de transfert peut gérer 60 opérations de disque simultanées, mais la bande passante réseau sera sûrement saturée avec un nombre inférieur. VMware a testé 20 opérations de disque simultanées, par exemple 20 clients téléchargeant un poste de travail local simultanément, avec une connexion réseau de plus de 1 Go par seconde.

Transfer Server Repository (Référentiel de Serveur de transfert)

Des images de base des postes de travail View Composer de clone lié sont conservées dans le Référentiel de Serveur de transfert, sur un partage de réseau. Plus vos disques de stockage réseau sont rapides, meilleures sont les performances.

Paramètres de pool

Utilisez View Composer pour créer des pools de postes de travail de clone lié. Lorsque vous utilisez l'assistant Créer un pool, choisissez une affectation dédiée et créez le pool uniquement pour les postes de travail prévus pour une utilisation en mode local. Les machines virtuelles en mode local peuvent être placées sur des magasins de données avec un IOPS inférieur au stockage prévu pour prendre en charge un nombre important de postes de travail View distants.

Réplication de données

Indiquez si les utilisateurs finaux doivent répliquer les données du disque du système d'exploitation, par exemple les données contenues dans une spécification de personnalisation. Dans le cas contraire, définissez une règle de façon à répliquer uniquement les disques persistants.

Si vous définissez un intervalle de réplication automatique, utilisez la valeur par défaut de 12 heures ou indiquez un intervalle inférieur.

N'activez pas la déduplication ni la compression, sauf si vous constatez des problèmes dus à une connexion réseau lente. Les fonctions de déduplication et de compression réduisent la quantité de bande passante réseau requise, aux dépens d'une puissance de traitement supérieure requise sur l'ordinateur de l'utilisateur final ou sur le Serveur de transfert.

Petit déploiement avec des dépenses minimales en capital

Vous pouvez réduire le nombre de serveurs ESX/ESXi requis pour le déploiement si vous augmentez le nombre de machines virtuelles sur chaque serveur.

Suivez les recommandations ci-dessous pour réduire la quantité de bande passante et le nombre d'opérations d'E/S requises par chaque machine virtuelle et pour augmenter le nombre de machines virtuelles sur un hôte ESX/ESXi.

- Définissez une règle de View obligeant les utilisateurs finaux à utiliser leurs postes de travail View en mode local uniquement. Avec ce paramètre, les machines virtuelles du datacenter restent verrouillées et désactivées.

- Définissez des règles de mode local empêchant les utilisateurs finaux d'initier une restitution, une restauration ou une réplication de postes de travail.
- Ne définissez aucun intervalle de réplication automatique.
- Configurez les paramètres de Serveur de connexion View de façon à empêcher l'utilisation de la déduplication et de la compression pour les opérations en mode local. Ces paramètres ne peuvent être utiles que si le réplication des données du poste de travail local se produit sur un réseau lent à un moment où l'utilisateur final constate une baisse des performances sur son ordinateur client.
- Configurez les paramètres de Serveur de connexion View de façon à empêcher l'utilisation de SSL pour les opérations ou l'approvisionnement en mode local.
- Utilisez View Composer pour créer des postes de travail de clone lié, mais n'utilisez pas la fonction de recomposition. Utilisez plutôt des mécanismes traditionnels de mise à jour logicielle pour déployer directement des correctifs et des mises à jour sur les postes de travail locaux, sur les ordinateurs des utilisateurs finaux.
- Si les performances de Serveur de connexion View sont affectées par le nombre de postes de travail locaux, définissez un intervalle de pulsation inférieur. La valeur par défaut est de six minutes.

Gestion de View Transfer Server

View Transfer Server est le composant View qui prend en charge des opérations de transfert de données pour des postes de travail locaux.

Comprendre View Transfer Server

View Transfer Server gère et rationalise des transferts de données entre le datacenter et des ordinateurs locaux. View Transfer Server est requis pour prendre en charge des postes de travail qui exécutent View Client with Local Mode.

View Transfer Server envoie des données entre les postes de travail distants et locaux dans plusieurs situations.

- Lorsqu'un utilisateur restitue ou emprunte un poste de travail, View Manager autorise et gère l'opération. View Transfer Server transfère les fichiers entre le datacenter et le poste de travail local.
- View Transfer Server synchronise des postes de travail locaux avec les postes de travail correspondants dans le datacenter en répliquant les modifications générées par l'utilisateur dans le datacenter.

  Les réplications se produisent à des intervalles que vous spécifiez dans des règles de mode local. Vous pouvez également initier des réplications dans View Administrator. Vous pouvez définir une règle qui permet aux utilisateurs d'initier des réplications depuis leurs postes de travail locaux.
- View Transfer Server distribue des données système communes à partir du datacenter vers les clients locaux. View Transfer Server télécharge des images de base de View Composer à partir du référentiel de Transfer Server vers des postes de travail locaux.

Un événement tel qu'une panne réseau ou le retrait de View Transfer Server de View Manager peut interrompre des transferts de données actifs. View Transfer Server reprend les transferts interrompus lorsque les composants sont de nouveau exécutés.

Ajouter Serveur de transfert View à View Manager

Serveur de transfert View fonctionne avec Serveur de connexion View pour transférer des fichiers et des données entre des postes de travail locaux et le datacenter. Avant que Serveur de transfert View puisse effectuer ces tâches, vous devez l'ajouter à votre déploiement de View Manager.

Vous pouvez ajouter plusieurs instances de Serveur de transfert View à View Manager. Les instances de Serveur de transfert View accèdent à un référentiel de Serveur de transfert commun. Ils partagent la charge de travail de transfert pour les postes de travail locaux gérés par une instance de Serveur de connexion View ou par un groupe d'instances de Serveur de connexion View répliquées.

Remarque Quand Serveur de transfert View est ajouté à View Manager, sa règle d'automatisation DRS (Distributed Resource Scheduler) est définie sur Manual (Manuel), ce qui désactive efficacement DRS.

Prérequis

- Vérifiez que Serveur de transfert View est installé sur une machine virtuelle Windows Server.
- Vérifiez que vCenter Server est ajouté à View Manager. La page **[Configuration de View] > [Serveurs]** dans View Administrator affiche les instances de vCenter Server qui sont ajoutées à View Manager.
- Si Serveur de transfert View est à la version 5.1 ou supérieure, et si vous prévoyez d'utiliser des postes de travail de clone lié en mode local, vérifiez que toutes les instances de Serveur de connexion View répliquées dans la configuration de View sont à la version 5.1 ou supérieure. Si une version antérieure de Serveur de connexion View envoie une demande pour publier une image de base au référentiel de Serveur de transfert, Serveur de transfert View ne peut pas effectuer l'opération de publication.

Procédure

1. Dans View Administrator, cliquez sur **[Configuration de View] > [Serveurs]** .
2. Cliquez sur l'onglet Transfer Servers (Serveurs de transfert) et cliquez sur **[Ajouter]** .
3. Dans l'assistant Add Serveur de transfert (Ajouter un serveur Serveur de transfert), sélectionnez l'instance de vCenter Server qui gère la machine virtuelle Serveur de transfert View et cliquez sur **[Suivant]** .
4. Sélectionnez la machine virtuelle où Serveur de transfert View est installé et cliquez sur **[Terminer]** .

   Serveur de connexion View reconfigure la machine virtuelle avec quatre contrôleurs SCSI. Plusieurs contrôleurs SCSI augmentent le nombre de transferts de disque que Serveur de transfert View peut effectuer simultanément.

Dans View Administrator, l'instance de Serveur de transfert View apparaît dans le volet Serveur de transferts (Serveurs Serveur de transfert). Si aucun référentiel de Serveur de transfert n'est configuré, l'état de Serveur de transfert View passe de **[En attente]** à **[Aucun référentiel de Serveur de transfert configuré]** . Si un référentiel de Serveur de transfert est configuré, l'état passe de **[En attente]** à **[Référentiel de Serveur de transfert en cours d'initialisation]** à **[Prêt]** .

Ce processus peut prendre plusieurs minutes. Vous pouvez cliquer sur le bouton d'actualisation dans View Administrator pour vérifier l'état actuel.

Lorsque l'instance de Serveur de transfert View est ajoutée à View Manager, le service Apache est démarré sur la machine virtuelle Serveur de transfert View.

Avertissement Si votre machine virtuelle Serveur de transfert View est une version antérieure à la version matérielle 7, vous devez configurer l'adresse IP statique sur la machine virtuelle Serveur de transfert View après avoir ajouté Serveur de transfert View à View Manager.

Lorsque plusieurs contrôleurs SCSI sont ajoutés à la machine virtuelle Serveur de transfert View, Windows supprime l'adresse IP statique et reconfigure la machine virtuelle pour utiliser DHCP. Une fois la machine virtuelle redémarrée, vous devez saisir de nouveau l'adresse IP statique dans la machine virtuelle.

Supprimer Serveur de transfert View de View Manager

Lorsque vous supprimez toutes les instances de Serveur de transfert View de View Manager, vous ne pouvez pas emprunter, restituer ou répliquer des données pour les postes de travail locaux.

Lorsque vous supprimez une instance de Serveur de transfert View effectuant des transferts, les opérations de transfert actif sont interrompues. Les sessions de poste de travail locales indiquent que l'état du transfert est interrompu.

Par exemple, si vous supprimez Serveur de transfert View alors que vous empruntez un poste de travail, l'opération d'emprunt est interrompue. L'utilisateur peut reprendre l'opération de transfert interrompue sur l'ordinateur client.

Remarque Vous devez supprimer une instance de Serveur de transfert View de View Manager avant d'effectuer les opérations suivantes :

- Désinstaller ou mettre à niveau une instance de Serveur de transfert View
- Effectuer des opérations de maintenance sur une machine virtuelle Serveur de transfert View dans vCenter Server

Procédure

1 Dans View Administrator, cliquez sur **[View Configuration (Configuration de View)] > [Servers (Serveurs)]** .

2 Cliquez sur l'onglet des serveurs Serveur de transfert et sélectionnez une instance de Serveur de transfert View.

3 Cliquez sur **[Remove (Supprimer)]** .

4 Si des transferts sont actuellement actifs, choisissez d'annuler les transferts actifs ou d'annuler cette tâche et de garder Serveur de transfert View.

5 Cliquez sur **[OK]** .

Lorsqu'une instance de Serveur de transfert View est supprimée de View Manager, sa règle d'automatisation DRS est réinitialisée sur la valeur définie avant l'ajout de Serveur de transfert View à View Manager.

Utiliser le mode de maintenance pour interrompre des transferts de données pour des postes de travail locaux

Lorsque vous placez une instance de Serveur de transfert View en mode de maintenance, vous interrompez des transferts de données actifs et empêchez les futurs transferts de données pour des postes de travail locaux sur cette instance de Serveur de transfert View. Lorsque vous quittez le mode de maintenance sur une instance de Serveur de transfert View, les transferts interrompus peuvent être repris à partir du client, et les futurs transferts peuvent avoir lieu.

Lorsque toutes les instances de Serveur de transfert View sont en mode de maintenance, vous pouvez migrer le référentiel de Serveur de transfert. Reportez-vous à la section « Migrer le référentiel de Serveur de transfert vers un nouvel emplacement », page 365.

Quand une instance de Serveur de transfert View est ajoutée à View Manager et est en mode actif, sa règle d'automatisation DRS est définie sur Manual (Manuel), ce qui désactive efficacement DRS. Pour migrer une instance de Serveur de transfert View vers un autre hôte ESX ou magasin de données, placez l'instance en mode de maintenance avant de commencer la migration.

Remarque Comme meilleure pratique, avant de mettre à jour ou de migrer des machines virtuelles qui peuvent être utilisées en mode local, placez Serveur de transfert View en mode de maintenance et vérifiez que tous les transferts de données sont terminés ou arrêtés. Par exemple, placez Serveur de transfert View en mode de maintenance avant d'utiliser Storage vMotion pour migrer des machines virtuelles complètes ou l'opération de rééquilibrage View Composer pour migrer des clones liés vers d'autres magasins de données. Cette pratique empêche les transferts de données en mode local lorsque des opérations de maintenance sont exécutées sur les machines virtuelles.

Procédure

1 Dans View Administrator, cliquez sur **[View Configuration (Configuration de View)] > [Servers (Serveurs)]** .

2 Cliquez sur l'onglet Transfer Servers (Serveurs de transfert) et sélectionnez une instance de Serveur de transfert View.

3 Cliquez sur **[Enter Maintenance Mode (Passer en mode de maintenance)]** .

4 Si des transferts sont actuellement actifs, choisissez d'annuler les transferts actifs ou attendez que les transferts actifs soient terminés avant de passer Serveur de transfert View en mode de maintenance.

   Si vous annulez des transferts actifs, Serveur de transfert View entre en mode de maintenance immédiatement.

   Si vous laissez les transferts en cours se terminer, Serveur de transfert View passe à l'état **[Maintenance Mode Pending (Mode de maintenance En attente)]** . Lorsque le transfert de disque en cours est terminé, Serveur de transfert View passe en mode de maintenance.

   Remarque Laisser les transferts actifs se terminer garantit que le disque actuel est transféré. Toutefois, des machines virtuelles contiennent plusieurs disques. Une opération de transfert, telle que l'emprunt d'un poste de travail, peut ne pas se terminer si aucune autre instance de Serveur de transfert View n'est disponible pour transférer les disques restants. Lorsqu'une instance de Serveur de transfert View est sortie du mode de maintenance, les transferts suspendus peuvent reprendre.

5 Cliquez sur **[OK]** .

Suivant

Lorsque vous êtes prêt à quitter le mode de maintenance de Serveur de transfert View, sélectionnez l'instance de Serveur de transfert View concernée et cliquez sur **[Exit Maintenance Mode (Quitter le mode de maintenance)]** . Les transferts interrompus peuvent être repris et de nouveaux transferts de données peuvent commencer.

État de View Transfer Server

View Transfer Server peut se trouver dans plusieurs états d'opération et de disponibilité. Dans View Administrator, vous pouvez suivre l'état de View Transfer Server dans le volet Transfer Servers (Serveurs Transfer Server) sur la page **[View Configuration (Configuration de View)] > [Servers (Serveurs)]** .

Tableau 14-1. États de View Transfer Server lors des opérations normales

État	Description
Ready (Prêt)	View Transfer Server et le référentiel de Transfer Server sont configurés et fonctionnent correctement.
Pending (En attente)	View Transfer Server est en train d'être ajouté à View Manager ou quitte le mode de maintenance. View Connection Server est en train d'établir activement une connexion avec View Transfer Server. Lorsque la connexion est faite, View Transfer Server passera dans un état opérationnel tel que Ready (Prêt).
Maintenance mode pending (En attente du mode de maintenance)	View Transfer Server entre en mode de maintenance tout en attendant que des transferts actifs et des opérations de publication de package se terminent.
Maintenance mode (Mode de maintenance)	Les transferts de données actifs sont interrompus. Les utilisateurs ne peuvent pas initier de nouveaux transferts. Les transferts planifiés en attente ne peuvent pas avoir lieu. View Transfer Server ne peut pas publier de packages sur le référentiel de Transfer Server.
Initializing Transfer Server repository (Initialisation du référentiel de Transfer Server)	View Transfer Server est en train d'initialiser le référentiel de Transfer Server. Si View Transfer Server a des difficultés à initialiser le référentiel de Transfer Server, l'état passera à un état d'erreur. Pour résoudre le problème, reportez-vous au conseil de dépannage correspondant à l'état d'erreur affiché.
No Transfer Server repository configured (Aucun référentiel de Transfer Server configuré)	Aucun référentiel de Transfer Server n'est configuré dans View Manager. Cet état n'indique pas une erreur car vous pouvez effectuer des opérations de transfert pour des machines virtuelles complètes sans configurer un référentiel de Transfer Server. Toutefois, cet état indique une erreur lorsque vous utilisez des postes de travail de clone lié en mode local. Vous ne pouvez pas effectuer des opérations de transfert pour des postes de travail de clone lié lorsque aucun référentiel de Transfer Server n'est configuré.

View Transfer Server passe à un état d'erreur lorsqu'il est indisponible ou ne peut fonctionner normalement. Pour résoudre le problème, reportez-vous au conseil de dépannage correspondant à l'état d'erreur affiché. Pour plus d'informations sur la configuration de connexions directes, reportez-vous à la section « Dépannage d'opérations de View Transfer Server et de poste de travail local », page 391.

Tableau 14-2. États d'erreur de View Transfer Server

État	Description
Bad Transfer Server repository (Mauvais référentiel de Transfer Server)	Le référentiel de Transfer Server auquel View Transfer Server doit se connecter est différent du référentiel de Transfer Server actuellement configuré dans View Connection Server.
Repository connection error (Erreur de connexion au référentiel)	View Transfer Server ne peut pas se connecter au référentiel de Transfer Server configuré.
Bad health check (Mauvaise vérification d'intégrité)	View Transfer Server n'a pas pu vérifier l'intégrité de View Manager. View Transfer Server est indisponible ou ne fonctionne pas correctement.

Tableau 14-2. États d'erreur de View Transfer Server (suite)

État	Description
Transfer Server repository conflict (Conflit de référentiel de Transfer Server)	Plusieurs instances de View Transfer Server sont configurées pour se connecter à différents référentiels de Transfer Server. Cet état se produit si plusieurs instances de View Transfer Server sont simultanément ajoutées à View Manager, et que chaque instance est configurée avec un référentiel de Transfer Server différent.
Web Server down (Serveur Web arrêté)	Le service Apache2.2 qui prend en charge le référentiel de Transfer Server n'est pas en cours d'exécution.

Gestion du référentiel de Transfer Server

View Transfer Server utilise le référentiel de Transfer Server pour stocker des images de base de View Composer téléchargées sur des postes de travail locaux. Le référentiel de Transfer Server est requis pour l'emprunt des postes de travail de clone lié pour qu'ils s'exécutent en mode local.

Utilisation du référentiel de Transfer Server pour télécharger des images système

Pour prendre en charge des postes de travail de clone lié exécutés en mode local, le référentiel de Transfer Server stocke des images de base View Composer dans un magasin de données accessible. View Manager et View Transfer Server approvisionnent et mettent à jour des postes de travail locaux de clone lié depuis le référentiel de Transfer Server.

Remarque Si vous n'utilisez pas de clone lié View Composer en mode local, inutile de configurer un référentiel de Transfer Server. Le référentiel de Transfer Server n'est pas utilisé pour les postes de travail de machine virtuelle complets qui s'exécutent en mode local.

Avant qu'un utilisateur puisse emprunter un poste de travail de clone lié afin qu'il s'exécute en mode local, vous devez publier son image de base sur le référentiel de Transfer Server.

Lorsque vous publiez un fichier d'image sur le référentiel de Transfer Server, View Transfer Server stocke les fichiers sous forme de packages cryptés. View Transfer Server peut compresser les packages pour rationaliser les téléchargements sur les postes de travail locaux.

Lorsqu'un utilisateur emprunte un poste de travail de clone lié pour la première fois, View Transfer Server effectue deux opérations :

- Il télécharge l'image de base depuis le référentiel de Transfer Server vers l'ordinateur local.
- Il télécharge le poste de travail de clone lié distant depuis le datacenter vers l'ordinateur local. Le poste de travail est constitué du disque delta du système d'exploitation du clone lié et d'un disque persistant de View Composer.

Lorsque vous exécutez des postes de travail de clone lié dans le datacenter, les clones liés partagent un accès à une image de base. Lorsque vous exécutez un poste de travail de clone lié en mode local, une copie de l'image de base doit résider avec le poste de travail de clone lié sur l'ordinateur local.

L'image de base n'est téléchargée qu'une seule fois si elle reste inchangée. Lorsque des utilisateurs restituent et empruntent de nouveau leurs postes de travail, View Transfer Server télécharge les disques delta du système d'exploitation du clone lié et les disques persistants de View Composer, pas l'image de base.

Si une image de base est recomposée, View Transfer Server télécharge l'image mise à jour depuis le référentiel de Transfer Server sur les ordinateurs locaux la prochaine fois que des utilisateurs empruntent leurs postes de travail. Pour plus d'informations, reportez-vous à la section « Recomposer des postes de travail de clone lié pouvant s'exécuter en mode local », page 294.

Important Un poste de travail de clone lié créé depuis une image de base doit être restitué dans le datacenter avant que vous puissiez le recomposer.

Déterminer la taille d'une image de base de View Composer

Le référentiel de Transfer Server doit être suffisamment volumineux pour stocker les images de base de View Composer pour tous les postes de travail de clone lié utilisés en mode local. Pour vous assurer que le référentiel de Transfer Server peut s'adapter à une image de base en particulier, vous pouvez déterminer la taille approximative de l'image de base.

La taille d'une image de base peut atteindre plusieurs gigaoctets.

La taille maximale d'une image de base est la somme des tailles approvisionnées des disques durs dans la machine virtuelle parente. Il est possible que la taille réelle de l'image de base soit inférieure au maximum.

Prérequis

Vérifiez que vous avez créé une machine virtuelle parente à utiliser pour créer un pool de postes de travail de clone lié.

Procédure

1 Dans vSphere Client, sélectionnez la machine virtuelle parente.

2 Cliquez sur **[Edit Settings (Modifier les paramètres)]** .

3 Sous l'onglet **[Hardware (Matériel)]** , sélectionnez le premier disque dur configuré.

Par exemple, sélectionnez **[Hard Disk 1 (Disque dur 1)]** .

4 Dans le volet Disk Provisioning (Approvisionnement de disque), lisez Provisioned Size (Taille approvisionnée).

5 Si la machine virtuelle contient plusieurs disques durs, répétez les étapes 3 et 4 pour chaque disque dur supplémentaire.

6 Ajoutez les tailles approvisionnées des disques durs.

Configurer le référentiel de Serveur de transfert

Le référentiel de Serveur de transfert stocke des images de base View Composer pour des postes de travail de clone lié qui s'exécutent en mode local. Pour donner à Serveur de transfert View l'accès au référentiel de Serveur de transfert, vous devez le configurer dans View Manager. Si vous n'utilisez pas de clones liés View Composer en mode local, vous n'avez pas à configurer un référentiel de Serveur de transfert.

Si Serveur de transfert View est configuré dans View Manager avant que vous ne configuriez le référentiel de Serveur de transfert, Serveur de transfert View valide l'emplacement du référentiel de Serveur de transfert lors de la configuration.

Si vous prévoyez d'ajouter plusieurs instances de Serveur de transfert View à ce déploiement de View Manager, configurez le référentiel de Serveur de transfert sur un partage de réseau. Les autres instances de Serveur de transfert View ne peuvent pas accéder à un référentiel de Serveur de transfert configuré sur un lecteur local sur une instance de Serveur de transfert View.

Si vous configurez un référentiel de Serveur de transfert distant sur un partage de réseau, vous devez fournir un ID d'utilisateur avec des informations d'identification pour accéder au partage de réseau. Pour améliorer la sécurité de l'accès au référentiel de Serveur de transfert, il est recommandé de limiter l'accès au réseau pour le référentiel aux View Administrators.

Prérequis

- Vérifiez que Serveur de transfert View est installé sur une machine virtuelle Windows Server.

- Vérifiez que Serveur de transfert View est ajouté à View Manager. Reportez-vous à la section « Ajouter Serveur de transfert View à View Manager », page 357.

REMARQUE L'ajout de Serveur de transfert View à View Manager avant de configurer le référentiel de Serveur de transfert est conseillé, il ne s'agit pas d'une obligation.

- Déterminez la taille du référentiel de Serveur de transfert pour stocker vos images de base de View Composer. La taille d'une image de base peut atteindre plusieurs gigaoctets. Pour déterminer la taille d'une image de base spécifique, reportez-vous à la section « Déterminer la taille d'une image de base de View Composer », page 362.

Procédure

1 Configurez un chemin et un dossier pour le référentiel de Serveur de transfert.

Le référentiel de Serveur de transfert peut se trouver sur un lecteur local ou un partage de réseau.

Option	Action
Local Transfer Server repository (Référentiel de Serveur de transfert local)	Sur la machine virtuelle sur laquelle Serveur de transfert View est installé, créez un chemin et un dossier pour le référentiel de Serveur de transfert. Par exemple : `C:\TransferRepository\`
Local Transfer Server repository (Référentiel de Serveur de transfert distant)	Configurez un chemin d'accès UNC pour le partage de réseau. Par exemple : `\\server.domain.com\TransferRepository\` Toutes les instances de Serveur de transfert View que vous ajoutez à ce déploiement de View Manager doivent avoir un accès réseau au lecteur partagé.

2 Dans View Administrator, cliquez sur **[View Configuration (Configuration de View)] > [Servers (Serveurs)]** .

3 Mettez toutes les instances de Serveur de transfert View en mode de maintenance.

a Cliquez sur l'onglet Transfer Servers de transfert et sélectionnez une instance de Serveur de transfert View.

b Cliquez sur **[Enter Maintenance Mode (Passer en mode de maintenance)]** et cliquez sur **[OK]** .

L'état de Serveur de transfert View passe sur **[Maintenance mode (Mode de maintenance)]** .

c Répétez l'Étape 3a et Étape 3b pour chaque instance.

Lorsque toutes les instances de Serveur de transfert View sont en mode de maintenance, les opérations de transfert actuelles sont arrêtées.

4 Dans le panneau du référentiel de Serveur de transfert, cliquez sur l'onglet General (Général) et sur **[Edit (Modifier)]** .

5 Saisissez l'emplacement du référentiel de Serveur de transfert et d'autres informations.

Option	Description
Partage de réseau	■ **[Path (Chemin d'accès)]** . Saisissez le chemin d'accès UNC que vous avez configuré. ■ **[User name (Nom d'utilisateur)]** . Saisissez l'ID d'utilisateur d'un administrateur avec des informations d'identification pour accéder au partage de réseau. ■ **[Password (Mot de passe)]** . Saisissez le mot de passe d'administrateur. ■ **[Domain (Domaine)]** . Saisissez le nom de domaine du partage de réseau au format NetBIOS. N'utilisez pas le suffixe `.com`.
Local Filesystem (Système de fichiers local)	Saisissez le chemin d'accès que vous avez configuré sur la machine virtuelle Serveur de transfert View locale.

6 Cliquez sur **[OK]** .

Si le chemin de réseau ou le lecteur local du référentiel est incorrect, la boîte de dialogue Edit Serveur de transfert Repository (Modifier le référentiel de Serveur de transfert) affiche un message d'erreur et ne vous permet pas de configurer l'emplacement. Vous devez saisir un emplacement valide.

7 Dans panneau des serveurs Serveur de transfert, sélectionnez l'instance de Serveur de transfert View et cliquez sur **[Exit Maintenance Mode (Quitter le mode de maintenance)]** .

L'état de Serveur de transfert View passe sur **[Ready (Prêt)]** .

Publier des fichiers de package dans le référentiel de Serveur de transfert

Avant qu'un utilisateur puisse emprunter un poste de travail de clone lié, vous devez publier son image de base View Composer sous forme de package dans le référentiel de Serveur de transfert.

Lorsqu'un utilisateur emprunte un poste de travail de clone lié, Serveur de transfert View télécharge les fichiers de package d'image de base du clone à partir du référentiel de Serveur de transfert vers l'ordinateur local.

Vous pouvez publier des packages à partir de la page **[Transfer Server repository (Référentiel de Serveur de transfert)]** dans View Administrator. Vous pouvez également publier des packages lorsque vous créez un pool de clone lié. Après la création d'un pool, vous pouvez également publier des packages à partir de la page du pool individuel à l'aide de l'option **[View Composer] > [Publish (Publier)]** .

Prérequis

- Vérifiez qu'une instance de Serveur de transfert View est configurée dans View Manager. Reportez-vous à la section « Ajouter Serveur de transfert View à View Manager », page 357.
- Si Serveur de transfert View correspond à la version 5.1 ou une version supérieure, vérifiez que toutes les instances de Serveur de connexion View dans la configuration View correspondent à la version 5.1 ou une version supérieure. Si une version antérieure de Serveur de connexion View envoie une demande de publication, Serveur de transfert View ne peut pas effectuer la publication.
- Vérifiez que le référentiel de Serveur de transfert est configuré dans View Manager. Reportez-vous à la section « Configurer le référentiel de Serveur de transfert », page 362.
- Vérifiez que le référentiel de Serveur de transfert est suffisamment volumineux pour s'adapter à l'image de base, qui peut atteindre plusieurs gigaoctets. Le référentiel doit avoir de l'espace pour l'image de base avant que les fichiers de package soient compressés. Reportez-vous à la section « Déterminer la taille d'une image de base de View Composer », page 362.
- Vérifiez qu'un pool de postes de travail de clone lié qui sera utilisé en mode local est créé.

Procédure

1 Dans View Administrator, cliquez sur **[View Configuration (Configuration de View)] > [Servers (Serveurs)]** .

2 Cliquez sur l'onglet des serveurs Serveur de transfert.

3 Dans le panneau du référentiel de Serveur de transfert, cliquez sur l'onglet Contents (Sommaire) et sur **[Publish (Publier)]** .

4 Sélectionnez une image de base View Composer dans la liste et cliquez sur **[OK]** . **[]**

Le package apparaît dans le volet Contents (Contenu) sur la page Serveur de transfert Repository (Référentiel de Serveur de transfert). L'état du package passe de **[Initializing (En cours d'initialisation)]** à **[Publishing (En cours de publication)]** à **[Published (Publié)]** .

Le processus de publication peut prendre plusieurs minutes. Cliquez sur l'icône d'actualisation de la page Transfer Repository (Référentiel de transfert) pour afficher la progression de l'opération en pourcentage.

Serveur de transfert View peut télécharger l'image de base View Composer publiée sur des postes de travail locaux.

Supprimer un fichier de package du référentiel de Serveur de transfert

Serveur de transfert View stocke des images de base View Composer sous forme de fichiers de package dans le référentiel de Serveur de transfert. Lorsque ces fichiers sont périmés ou qu'ils ne sont plus utilisés, vous pouvez supprimer les packages du référentiel de Serveur de transfert.

Vous pouvez supprimer un fichier de package même si des postes de travail de clone lié utilisent toujours l'image de base à partir de laquelle le fichier de package a été publié. Une fois le fichier de package supprimé, ces postes de travail ne peuvent pas être empruntés.

Prérequis

- Vérifiez que Serveur de transfert View est configuré dans View Manager. Reportez-vous à la section « Ajouter Serveur de transfert View à View Manager », page 357.
- Vérifiez qu'un référentiel de Serveur de transfert est configuré. Reportez-vous à la section « Configurer le référentiel de Serveur de transfert », page 362.

Procédure

1. Dans View Administrator, cliquez sur **[View Configuration (Configuration de View)] > [Servers (Serveurs)]** .
2. Cliquez sur l'onglet Serveur de transfert.
3. Dans le panneau du référentiel de Serveur de transfert, cliquez sur l'onglet Contents (Sommaire) et sélectionnez un fichier de package.
4. Cliquez sur **[Delete (Supprimer)]** .

   Une boîte de dialogue vous alerte si des postes de travail de clone lié utilisent l'image de base à partir de laquelle le fichier de package sélectionné a été publié. Vous pouvez annuler la suppression du package ou continuer.
5. Cliquez sur **[OK]** .

Le package passe à l'état **[Pending Delete (Suppression en attente)]** et est supprimé.

Migrer le référentiel de Serveur de transfert vers un nouvel emplacement

Vous pouvez migrer le référentiel de Serveur de transfert vers un nouvel emplacement si votre disque dur actuel ne contient pas suffisamment d'espace.

Toutes les instances de Serveur de transfert View associées à un serveur Serveur de connexion View doivent être en mode de maintenance pour que vous puissiez migrer le référentiel de Serveur de transfert.

Si vous possédez plusieurs instances de Serveur de transfert View, migrez le référentiel de Serveur de transfert vers un lecteur partagé de réseau. Les autres instances de Serveur de transfert View ne peuvent pas accéder à un référentiel de Serveur de transfert configuré sur un lecteur local sur une instance de Serveur de transfert View.

Prérequis

- Vérifiez que Serveur de transfert View est installé et configuré. Reportez-vous à la section « Ajouter Serveur de transfert View à View Manager », page 357.

- Ne publiez pas de packages dans le référentiel de Serveur de transfert lorsque vous migrez le référentiel. Si un package est publié dans le référentiel actuel une fois que vous avez commencé à copier les fichiers du référentiel dans le nouvel emplacement, il est possible que le package ne soit pas copié dans le nouvel emplacement.

  Pour respecter cette condition préalable, vous pouvez mettre Serveur de transfert View en mode de maintenance avant de copier manuellement le référentiel, mais cette approche allongera le temps d'arrêt des transferts de données lors de la copie des fichiers du référentiel.

  Au lieu de cela, cette procédure vous indique que vous devez copier les fichiers du référentiel avant de mettre Serveur de transfert View en mode de maintenance. Cette approche réduit le temps d'indisponibilité de Serveur de transfert View.

Procédure

1 Configurez un dossier de destination local ou à distance vers lequel vous migrerez le référentiel de Serveur de transfert.

Option	Action
Local Transfer Server repository (Référentiel de Serveur de transfert local)	Sur la machine virtuelle sur laquelle Serveur de transfert View est installé, créez un chemin et un dossier pour le référentiel de Serveur de transfert. Par exemple : `C:\TransferRepository\`
Remote Transfer Server repository (Référentiel de Serveur de transfert distant)	Configurez un chemin d'accès UNC pour le partage de réseau. Par exemple : `\\server.domain.com\TransferRepository\` Toutes les instances de Serveur de transfert View que vous ajoutez à ce déploiement de View Manager doivent avoir un accès réseau au lecteur partagé.

2 Copiez manuellement le répertoire racine du référentiel de Serveur de transfert vers l'emplacement de destination.

  Vous devez copier tout le répertoire racine, pas uniquement les fichiers de package qui résident sous le répertoire racine.

3 Dans View Administrator, cliquez sur **[View Configuration (Configuration de View)] > [Servers (Serveurs)]** .

4 Mettez toutes les instances de Serveur de transfert View en mode de maintenance.

  a Cliquez sur l'onglet des serveurs Serveur de transfert et sélectionnez une instance de Serveur de transfert View.

  b Cliquez sur **[Enter Maintenance Mode (Passer en mode de maintenance)]** et cliquez sur **[OK]** .

    L'état de Serveur de transfert View passe sur **[Maintenance]** .

  c Répétez ces étapes pour chaque instance :

  Lorsque toutes les instances de Serveur de transfert View sont en mode de maintenance, les opérations de transfert actuelles sont arrêtées.

5 Dans le panneau du référentiel de Serveur de transfert, cliquez sur l'onglet General (Général) et sur **[Edit (Modifier)]** .

6 Saisissez l'emplacement du référentiel de Serveur de transfert de destination et d'autres informations.

Option	Description
Partage de réseau	■ **[Path (Chemin d'accès)]** . Saisissez le chemin d'accès UNC que vous avez configuré. ■ **[User Name (Nom d'utilisateur)]** . Saisissez l'ID d'utilisateur d'un administrateur avec des informations d'identification pour accéder au partage de réseau. ■ **[Password (Mot de passe)]** . Saisissez le mot de passe d'administrateur. ■ **[Domain (Domaine)]** . Saisissez le nom de domaine du partage de réseau au format NetBIOS. N'utilisez pas le suffixe `.com`.
Local filesystem (Système de fichiers local)	Saisissez le chemin d'accès que vous avez configuré sur la machine virtuelle Serveur de transfert View locale.

7 Cliquez sur **[OK]** .

8 Dans panneau des serveurs Serveur de transfert, sélectionnez l'instance de Serveur de transfert View et cliquez sur **[Exit Maintenance Mode (Quitter le mode de maintenance)]** et sur **[OK]**

L'état de Serveur de transfert View passe sur **[Ready (Prêt)]** .

9 (Facultatif) Supprimez manuellement les fichiers de package du dossier du référentiel de Serveur de transfert d'origine.

Restaurer d'un dossier de référentiel de Serveur de transfert corrompu

Si le dossier partagé de réseau ou le dossier local sur lequel le référentiel de Serveur de transfert est configuré devient corrompu, vous devez recréer le référentiel de Serveur de transfert sur un dossier qui fonctionne.

Cette situation se produit si le partage de réseau ou le lecteur local est inaccessible et que vous ne pouvez pas accéder aux fichiers de package de Serveur de transfert qui sont stockés dans le dossier configuré. Dans ce cas, vous ne pouvez pas copier manuellement les fichiers de package du dossier corrompu vers un nouveau dossier.

Prérequis

- Familiarisez-vous avec la configuration d'un référentiel de Serveur de transfert. Reportez-vous à la section « Configurer le référentiel de Serveur de transfert », page 362.
- Familiarisez-vous avec la suppression et l'ajout de Serveur de transfert View dans View Manager et avec le passage de Serveur de transfert View en mode de maintenance. Reportez-vous à la section « Gestion de View Transfer Server », page 356.
- Familiarisez-vous avec la publication et la suppression de packages dans le référentiel de Serveur de transfert. Reportez-vous à la section « Publier des fichiers de package dans le référentiel de Serveur de transfert », page 364 et « Supprimer un fichier de package du référentiel de Serveur de transfert », page 365.

Procédure

1 Supprimez toutes les instances de Serveur de transfert View de View Manager.

2 Configurez un nouveau chemin et un nouveau dossier pour un partage de réseau ou un lecteur local.

Suivez la même procédure que vous utilisez lorsque vous créez un nouveau référentiel de Serveur de transfert.

3 Ajouter les instances de Serveur de transfert View à View Manager.

4 Placez les instances de Serveur de transfert View en mode de maintenance.

5 Configurez le référentiel de Serveur de transfert dans View Manager, en spécifiant le nouveau partage du réseau ou le chemin local.

Serveur de transfert View valide le nouveau chemin du référentiel de Serveur de transfert. L'état de chaque package est **[Missing Package (Package manquant)]** .

6 Rétablissez chaque instance de Serveur de transfert View sur un état **[Ready (Prêt)]** en quittant le mode de maintenance.

7 Supprimez les packages déplacés du référentiel de Serveur de transfert.

8 Republiez les packages dans le référentiel de Serveur de transfert.

Utilisez les machines virtuelles parentes et les snapshots d'origine pour publier les images de base de View Composer en tant que packages dans le référentiel.

Gestion des transferts de données

Vous pouvez définir des règles pour configurer des réplications et optimiser des opérations de transfert. Vous pouvez également initier des demandes de réplication entre des réplications planifiées. Si nécessaire, vous pouvez restaurer un poste de travail pour ignorer la version empruntée en local.

Les réplications se produisent en séquence pour conserver l'intégrité des données de poste de travail local.

Chaque réplication transfère des données depuis un snapshot pris du poste de travail local lorsque la réplication démarre. Par conséquent, chaque réplication représente un état différent du poste de travail local.

Lorsque vous initiez une réplication, ou lorsqu'une réplication est planifiée pour démarrer, la demande démarre la prochaine fois que l'ordinateur client contacte le datacenter. View Client with Local Mode prend un snapshot et démarre la réplication.

View ne conserve qu'une réplication en attente à la fois.

Remarque Au début et à la fin de chaque réplication, l'utilisateur final peut remarquer que les performances du poste de travail sont affectées pendant quelques secondes quand un snapshot local est pris ou mis à jour.

- Définir des règles de réplication page 369

  La réplication synchronise des postes de travail locaux avec leurs postes de travail distants correspondants en envoyant des modifications générées par l'utilisateur au datacenter. Vous pouvez définir des règles pour configurer la fréquence de réplication, pour autoriser des utilisateurs à différer des réplications et pour sélectionner le type de disque de clone lié à répliquer.

- Initier des réplications de postes de travail locaux page 370

  Vous pouvez initier des réplications pour des postes de travail exécutés en mode local. Votre demande peut démarrer une réplication avant la prochaine réplication planifiée. Si la règle client l'autorise, un utilisateur final qui a emprunté un poste de travail local peut également initier une réplication depuis View Client.

- Restaurer un poste de travail emprunté en local page 370

  Si un utilisateur final perd un ordinateur portable contenant un poste de travail local, ou si le disque dur est endommagé, vous pouvez restaurer le poste de travail View de façon à ce que l'utilisateur final puisse emprunter le poste de travail sur un autre ordinateur. Si la règle client l'autorise, un utilisateur final qui a emprunté un poste de travail local peut également restaurer le poste de travail depuis View Client.

- Supprimer un poste de travail local page 371

  Lorsque vous restaurez un poste de travail local ou désinstallez View Client, les fichiers composant un poste de travail local sur cet ordinateur client ne sont pas supprimés ou effacés. Pour supprimer un poste de travail local, vous devez supprimer manuellement ses fichiers.

Définir des règles de réplication

La réplication synchronise des postes de travail locaux avec leurs postes de travail distants correspondants en envoyant des modifications générées par l'utilisateur au datacenter. Vous pouvez définir des règles pour configurer la fréquence de réplication, pour autoriser des utilisateurs à différer des réplications et pour sélectionner le type de disque de clone lié à répliquer.

Vous configurez des fonctions de réplication en définissant des règles du mode local. Pour voir des descriptions, reportez-vous à la section « Règles du mode local », page 204.

Prérequis

Déterminez de définir ces règles globalement, pour des pools de postes de travail individuels, et pour des utilisateurs individuels. Pour plus d'informations, reportez-vous à la section « Définition de règles dans View Administrator », page 201.

Procédure

- Définissez l'option **[Target replication frequency (Fréquence de réplication cible)]** .

  Cette règle spécifie l'intervalle en jours, heures ou minutes entre le début d'une réplication et le début de la réplication suivante. Vous pouvez interdire les réplications planifiées en sélectionnant **[No replication (Aucune réplication)]** .

  La règle **[No replication (Aucune réplication)]** n'interdit pas les demandes de réplication explicites. Vous pouvez initier des réplications dans View Administrator, et les utilisateurs peuvent demander des réplications si la règle **[User initiated replication (Réplication initiée par l'utilisateur)]** est définie sur **[Allow (Autoriser)]** .

  Si une réplication dure plus longtemps que l'intervalle spécifié dans la règle **[Target replication frequency (Fréquence de réplication cible)]** , la prochaine réplication planifiée démarre après la fin de la précédente. La réplication en attente n'annule pas la précédente.

  Par exemple, la règle **[Target replication frequency (Fréquence de réplication cible)]** doit être définie sur un jour. Une réplication peut commencer à midi le mardi. Si l'ordinateur client est déconnecté du réseau, la réplication peut durer plus de 24 heures. À midi le mercredi, View Client with Local Mode démarre la prochaine demande de réplication. Après la fin de la réplication précédente, View Client with Local Mode prend un snapshot et démarre la réplication en attente.

- Définissez l'option **[User deferred replication (Réplication différée par l'utilisateur)]** .

  Cette règle autorise un utilisateur à interrompre une réplication en cours. La réplication ne reprend pas, et aucune nouvelle réplication ne démarre, jusqu'à la fin de la période de report. La période de report est de deux heures.

- Définissez l'option **[Disks replicated (Disques répliqués)]** .

  Cette règle détermine si vous voulez répliquer uniquement des disques persistants de View Composer, des disques du système d'exploitation ou à la fois des disques du système d'exploitation et des disques persistants. Cette règle n'affecte que les postes de travail de clone lié.

  Cette règle est définie lorsqu'un poste de travail est emprunté. Si vous modifiez la règle, la modification prend effet quand le poste de travail est de nouveau emprunté.

- Définissez l'option **[User initiated replication (Réplication initiée par l'utilisateur)]** .

  Cette règle autorise un utilisateur à demander une réplication depuis un poste de travail local.

Initier des réplications de postes de travail locaux

Vous pouvez initier des réplications pour des postes de travail exécutés en mode local. Votre demande peut démarrer une réplication avant la prochaine réplication planifiée. Si la règle client l'autorise, un utilisateur final qui a emprunté un poste de travail local peut également initier une réplication depuis View Client.

Si vous initiez une réplication quand View Client with Local Mode est déjà en train de répliquer des données, votre réplication démarre après la fin de la réplication précédente. Votre demande en attente n'abandonne pas la réplication précédente.

Procédure

1 Dans View Administrator, cliquez sur **[Monitoring (Contrôle)] > [Local Sessions (Sessions locales)]** .

2 Sélectionnez des postes de travail locaux.

3 Cliquez sur **[Initiate Replication (Initier la réplication)]** .

4 Choisissez de démarrer la réplication lors de la prochaine connexion entre le poste de travail local et le datacenter.

Option	Description
Oui	Démarre la réplication la prochaine fois que View Client est exécuté et que le poste de travail contacte le datacenter.
Non	Annule la demande de réplication. Si vous avez demandé une réplication précédemment et qu'elle n'a pas encore démarré, vous pouvez sélectionner **[No (Non)]** pour annuler la réplication en attente.

5 Cliquez sur **[OK]** .

La réplication démarre la prochaine fois que View Client est exécuté et que l'ordinateur client contacte le datacenter. Si une réplication est déjà active, votre réplication démarre lorsque la réplication précédente est terminée.

Suivant

Si vous avez initié la réplication car vous avez besoin que le poste de travail soit restitué sans interaction de l'utilisateur final, vous pouvez restaurer le poste de travail local quand la réplication est terminée. Reportez-vous à la section « Restaurer un poste de travail emprunté en local », page 370.

Restaurer un poste de travail emprunté en local

Si un utilisateur final perd un ordinateur portable contenant un poste de travail local, ou si le disque dur est endommagé, vous pouvez restaurer le poste de travail View de façon à ce que l'utilisateur final puisse emprunter le poste de travail sur un autre ordinateur. Si la règle client l'autorise, un utilisateur final qui a emprunté un poste de travail local peut également restaurer le poste de travail depuis View Client.

Si un administrateur démarre une opération de restauration, le client effectue l'une des actions suivantes :

- Si l'utilisateur a ouvert une session sur le poste de travail emprunté, la session est fermée dès que View Client reçoit une notification. L'utilisateur ne peut plus ouvrir de session sur le poste de travail emprunté.
- Si la session de l'utilisateur n'est pas ouverte, les prochaines tentatives de connexion sont redirigées vers la copie en ligne du poste de travail. Pour continuer à travailler en mode local, l'utilisateur doit maintenant emprunter le poste de travail à partir du serveur.

Prérequis

Si un administrateur veut conserver les données les plus récentes du poste de travail local, effectuez une opération de réplication. Reportez-vous à la section « Initier des réplications de postes de travail locaux », page 370.

IMPORTANT Si vous effectuez une réplication, vous devez attendre la fin de la réplication avant d'initier une opération de restauration. Les restaurations ne sont pas placées dans une file d'attente derrière les autres opérations. Pour savoir si une réplication est terminée, dans View Administrator, cliquez sur **[Monitoring (Contrôle)] > [Local Sessions (Sessions locales)]** et notez l'heure à laquelle la dernière réplication s'est terminée.

Procédure

- Sélectionnez l'option **[Rollback (Restaurer)]** .

Option	Action
Utilisateur de View Administrator	Dans View Administrator, sélectionnez **[Monitoring (Contrôle)] > [Local Sessions (Sessions locales)]** , sélectionnez le poste de travail et cliquez sur **[Rollback (Restaurer)]** .
Utilisateur final	Si vous êtes un utilisateur autorisé sur le poste de travail, dans View Client, cliquez avec le bouton droit sur le poste de travail dans la liste des postes de travail disponibles et sélectionnez **[Rollback (Restaurer)]** . L'option **[Rollback (Restaurer)]** n'est disponible que si la règle de poste de travail client l'autorise.

La version empruntée du poste de travail est ignorée. Un utilisateur doit de nouveau emprunter la version en ligne pour pouvoir utiliser le poste de travail en mode local.

Suivant

Pour nettoyer les fichiers sur l'ordinateur de l'utilisateur final, demandez à ce dernier de supprimer le répertoire de mode local pour ce poste de travail. Reportez-vous à la section « Supprimer un poste de travail local », page 371.

Pour plus d'informations sur l'emprunt d'un poste de travail View pour une utilisation en mode local, consultez le document *Installation de View*.

Supprimer un poste de travail local

Lorsque vous restaurez un poste de travail local ou désinstallez View Client, les fichiers composant un poste de travail local sur cet ordinateur client ne sont pas supprimés ou effacés. Pour supprimer un poste de travail local, vous devez supprimer manuellement ses fichiers.

Prérequis

Vérifiez que le poste de travail local n'est plus emprunté. Si le poste de travail local contient des données qui n'ont pas été répliquées sur le poste de travail View résidant dans le datacenter, demandez à l'utilisateur final de restituer le poste de travail. Si la restitution du poste de travail n'est pas possible, utilisez View Administrator pour répliquer les données. Reportez-vous à la section « Initier des réplications de postes de travail locaux », page 370.

Procédure

- Sur l'ordinateur client, sélectionnez et supprimez le dossier contenant les fichiers qui composent le poste de travail local que vous souhaitez supprimer.

  Le dossier réside dans le répertoire d'emprunt du poste de travail local. Lors du téléchargement de votre premier poste de travail local, si vous n'avez pas cliqué sur **[Options]** et modifier le répertoire de stockage des postes de travail locaux, ces derniers sont stockés dans le répertoire d'emprunt défini par défaut.

Système d'exploitation du poste de travail	Répertoire d'emprunt par défaut
Répertoire par défaut sur Windows 8, Windows 7 et Windows Vista	`C:\Users\`*`User Name`*`\AppData\Local\VMware\VDM\Local Desktops\`*`pool_display_name`*
Répertoire par défaut sur Windows XP	`C:\Documents and Settings\`*`User Name`*`\Local Settings\Application Data\VMware\VDM\Local Desktops\`*`pool_display_name`*

  Le répertoire `AppData` des systèmes d'exploitation Windows 8 et Windows 7 est un dossier masqué. Vous devrez peut-être afficher ce dossier masqué pour accéder aux fichiers du poste de travail local.

Configurer la sécurité et l'optimisation pour des opérations de poste de travail local

Vous pouvez configurer des communications tunnel et le chiffrement SSL pour des opérations du poste de travail local. Vous pouvez également optimiser des transferts de données entre les ordinateurs locaux et le datacenter.

Ces paramètres sont spécifiques à une instance de Serveur de connexion View. Vous pouvez activer ces paramètres sur une instance aux utilisateurs de poste de travail local qui se connectent à partir d'Internet, mais désactivez les paramètres sur une instance dédiée aux utilisateurs internes n'utilisant pas de poste de travail local.

Prérequis

- Familiarisez-vous avec les paramètres SSL et de communications tunnel pour les opérations de poste de travail local. Reportez-vous à la section « Définition d'options de sécurité pour des opérations de poste de travail local », page 373.
- Familiarisez-vous avec l'utilisation de la déduplication et de la compression pour optimiser les transferts de données sur le réseau. Reportez-vous à la section « Optimisation des transferts de données entre des ordinateurs hôte de poste de travail local et le datacenter », page 373.

Procédure

1. Dans View Administrator, cliquez sur **[View Configuration (Configuration de View)] > [Servers (Serveurs)]** .
2. Cliquez sur l'onglet des serveurs Serveur de connexion View, sélectionnez une instance de Serveur de connexion View et cliquez sur **[Edit (Modifier)]** .
3. Dans la boîte de modification des paramètres Serveur de connexion View, cliquez sur l'onglet Local (Mode local).
4. Sélectionnez des paramètres de sécurité et d'optimisation pour les transferts de données et les opérations de poste de travail local.

Optimisation des transferts de données entre des ordinateurs hôte de poste de travail local et le datacenter

Vous pouvez réduire la quantité de données envoyées sur le réseau au cours d'opérations de transfert entre les ordinateurs client qui hébergent des postes de travail locaux et le datacenter. Vous utilisez la déduplication et la compression pour optimiser les transferts de données.

Tableau 14-3 montre les paramètres de déduplication et de compression pour les transferts de données.

Les opérations de transfert incluent la restitution et l'emprunt de postes de travail, la réplication de données depuis des postes de travail locaux vers le datacenter et le téléchargement d'images système sur des postes de travail locaux.

Pour déterminer l'impact de la déduplication et de la compression sur les transferts de données, consultez les journaux View Client with Local Mode. Reportez-vous à la section « Déterminer les effets de la déduplication et de la compression sur les transferts de données », page 376.

Tableau 14-3. Paramètres de déduplication et de compression pour des transferts de données

Paramètre	Description
[Use deduplication for Local Mode operations (Utiliser la déduplication pour des opérations en mode local)]	Évite l'envoi de données redondantes des ordinateurs client vers le datacenter. La déduplication fonctionne sur des transferts de l'ordinateur client vers le datacenter, y compris des réplications et des restitutions de poste de travail. La déduplication n'a pas lieu lorsque des postes de travail sont empruntés. Avec la déduplication, l'ordinateur client détecte des blocs identiques de données et envoie une référence du bloc d'origine au lieu d'envoyer de nouveau l'intégralité du bloc. La déduplication est intéressante sur les réseaux lents car elle économise de la bande passante réseau. Toutefois, la déduplication peut s'ajouter à la charge de travail de CPU sur l'ordinateur client lorsqu'elle recherche des blocs de données identiques et à la charge de travail d'E/S sur View Transfer Server lorsqu'elle lit des blocs en double sur le disque. Sur les réseaux rapides, il est conseillé de désactiver la déduplication. Il est conseillé par défaut de ne pas utiliser la déduplication.
[Use compression for Local Mode operations (Utiliser la compression pour des opérations en mode local)]	Compresse des fichiers d'image système et de poste de travail avant de les envoyer sur le réseau. Comme la déduplication, la compression économise de la bande passante et accélère les transferts sur les réseaux lents. Toutefois, View Transfer Server utilise des ressources informatiques supplémentaires pour compresser les fichiers. Lorsque vous décidez d'utiliser la compression, vous devez comparer les avantages en termes de performances réseau et les coûts liés à l'environnement serveur. Il est conseillé par défaut de ne pas utiliser la compression.

Définition d'options de sécurité pour des opérations de poste de travail local

Vous pouvez définir le niveau de sécurité d'opérations de transfert en utilisant le chiffrement SSL et des connexions par tunnel entre les ordinateurs client qui hébergent des postes de travail locaux et le datacenter.

Tableau 14-4 montre les paramètres de sécurité pour les opérations du poste de travail local. Le fait de ne pas utiliser SSL ou de connexion par tunnel augmente la vitesse du transfert de données aux dépens de la communication de données sécurisées.

Les paramètres SSL n'affectent pas les données locales sur les ordinateurs client, qui sont toujours cryptées.

Le disque de données stocké localement sur des systèmes client est chiffré avec un niveau de chiffrement par défaut de AES-128. Les clés de chiffrement sont stockées sur le système client, chiffrées avec une clé dérivée d'un hachage des informations d'identification de l'utilisateur (nom d'utilisateur et mot de passe ou carte à puce et code PIN). Du côté serveur, la clé est stockée dans View LDAP. Les mesures de sécurité que vous utilisez pour protéger View LDAP sur le serveur protègent également les clés de chiffrement en mode local stockées dans LDAP.

Tableau 14-4. Utilisation d'une connexion par tunnel sécurisée et de SSL pour des opérations du poste de travail local

Paramètre	Description
[Utiliser une connexion par tunnel sécurisée pour des opérations en mode local]	Détermine si les postes de travail locaux utilisent des communications par tunnel. Si ce paramètre est activé, le trafic du réseau est routé via Serveur de connexion View ou un serveur de sécurité, si un serveur de ce type est configuré. Si ce paramètre est désactivé, les transferts de données ont lieu directement entre des postes de travail locaux et Serveur de transfert View. Ce paramètre est désactivé par défaut.
[Utiliser SSL pour des opérations en mode local]	Détermine si les communications et les transferts de données entre des ordinateurs client et le datacenter utilisent le chiffrement SSL. Ces opérations comprennent la restitution et l'emprunt de postes de travail et la réplication de données depuis des ordinateurs client vers le datacenter, mais n'incluent pas les transferts d'images de base de View Composer. Ces opérations impliquent des connexions entre des ordinateurs client et Serveur de transfert View. Ce paramètre est activé par défaut.
[Utiliser SSL lors de l'approvisionnement de postes de travail en mode local]	Détermine si les transferts de fichiers d'image de base View Composer depuis le référentiel de Serveur de transfert vers des ordinateurs client utilisent le chiffrement SSL. Ces opérations impliquent des connexions entre des ordinateurs client et Serveur de transfert View. Ce paramètre est activé par défaut.

Modifier le cryptage de clé de chiffrement du poste de travail local pour la génération de nouvelles clés

Par défaut, Serveur de connexion View utilise AES-128 pour chiffrer le fichier de disque virtuel (`.vmdk`) lorsque des utilisateurs restituent et empruntent un poste de travail local. Si vous préférez un chiffrement renforcé, vous pouvez modifier le cryptage de clé de chiffrement sur AES-192 ou AES-256 en modifiant une propriété générale dans View LDAP sur votre hôte de Serveur de connexion View.

Quand vous avez modifié le cryptage de clé de chiffrement pour des postes de travail locaux, le nouveau cryptage est utilisé pour la génération de nouvelles clés, par exemple, lorsqu'un poste de travail local est emprunté pour la première fois. Les clés générées précédemment ne sont pas modifiées. Pour modifier le cryptage de clé de chiffrement pour des postes de travail locaux existants, reportez-vous à la section « Modifier le cryptage de clé de chiffrement pour un poste de travail local existant », page 375.

Vous utilisez l'utilitaire ADSI Edit pour modifier View LDAP. L'utilitaire ADSI Edit est installé avec Serveur de connexion View. Lorsque vous modifiez View LDAP sur une instance de Serveur de connexion View, la modification est propagée à toutes les instances de Serveur de connexion View.

Prérequis

Pour plus d'informations sur l'utilisation de l'utilitaire ADSI Edit sur votre version du système d'exploitation Windows, consultez le site Web Microsoft TechNet.

Procédure

1 Démarrez l'utilitaire ADSI Edit sur votre hôte de Serveur de connexion View.

2 Dans la boîte de dialogue des paramètres de connexion, sélectionnez ou connectez-vous à **[DC=vdi, DC=vmware, DC=int]** .

3 Dans le volet Computer (Ordinateur), sélectionnez ou tapez **`localhost:389`** ou le nom de domaine complet qualifié (FQDN) de l'hôte de Serveur de connexion View suivi du port 389.

Par exemple : **`localhost:389`** ou **`mycomputer.mydomain.com:389`**

4 Sur l'objet **[CN=Common, OU=Global, OU=Properties]** , définissez l'attribut **[pae-OVDIKeyCipher]** sur la nouvelle valeur de cryptage de clé de chiffrement.

Vous pouvez définir la valeur de cryptage de clé de chiffrement sur **`AES-128`**, **`AES-192`** ou **`AES-256`**. La valeur par défaut est **`AES-128`**.

Modifier le cryptage de clé de chiffrement pour un poste de travail local existant

Pour modifier le cryptage de clé de chiffrement pour un poste de travail local existant, vous modifiez l'enregistrement **[pae-VM]** pour le poste de travail local dans View LDAP sur votre hôte de Serveur de connexion View.

Vous utilisez l'utilitaire ADSI Edit pour modifier View LDAP. L'utilitaire ADSI Edit est installé avec Serveur de connexion View. Lorsque vous modifiez View LDAP sur une instance de Serveur de connexion View, la modification est propagée à toutes les instances de Serveur de connexion View.

Prérequis

- Modifiez le cryptage de clé de chiffrement pour des postes de travail locaux. Reportez-vous à la section « Modifier le cryptage de clé de chiffrement du poste de travail local pour la génération de nouvelles clés », page 374.
- Pour plus d'informations sur l'utilisation de l'utilitaire ADSI Edit sur votre version du système d'exploitation Windows, consultez le site Web Microsoft TechNet.

Procédure

1 Si le poste de travail local est emprunté, restituez-le et supprimez tous les fichiers locaux existants.

2 Démarrez l'utilitaire ADSI Edit sur votre hôte de Serveur de connexion View.

3 Dans la boîte de dialogue des paramètres de connexion, sélectionnez ou connectez-vous à **[DC=vdi, DC=vmware, DC=int]** .

4 Dans le volet Computer (Ordinateur), sélectionnez ou tapez **`localhost:389`** ou le nom de domaine complet qualifié (FQDN) de l'hôte de Serveur de connexion View suivi du port 389.

Par exemple : **`localhost:389`** ou **`mycomputer.mydomain.com:389`**

5 Dans l'enregistrement **[pae-VM]** pour le poste de travail local, effacez les valeurs pour les attributs **[pae-mVDIOfflineAuthKey]** , **[pae-mVDIOfflineDataKey]** et **[pae-mVDIOfflineObfuscationKey]** .

6 Empruntez le poste de travail local.

Serveur de connexion View génère de nouvelles clés pour le poste de travail local. Les nouvelles clés ont la nouvelle valeur de cryptage de clé de chiffrement.

Déterminer les effets de la déduplication et de la compression sur les transferts de données

Vous pouvez indiquer dans quelle mesure la déduplication et la compression réduisent la quantité de données envoyée sur le réseau lors des opérations de transfert. Pour connaître la taille des transferts de données, lisez les journaux View Client with Local Mode sur l'ordinateur client.

Lors d'une restitution ou d'une réplication, le poste de travail local affiche la quantité de données qui serait transférée dans le datacenter du poste de travail distant si aucune optimisation n'était effectuée. Cette quantité ne reflète pas les données véritablement envoyées sur le réseau. Le même nombre apparaît, que la déduplication et la compression soient activées ou non.

Lorsque les deux fonctions sont activées, View Client commence par utiliser la déduplication pour supprimer les blocs de données redondantes des données qui seront transférées. Ensuite, View Client compresse les données restantes ou indique que les données ne peuvent pas être compressées.

Lire les journaux View Client with Local Mode

Pour générer des entrées de journal affichant des statistiques de déduplication et de compression, vous devez sélectionner le mode `débogage` pour les journaux.

Tableau 14-5 indique l'emplacement des journaux View Client with Local Mode sur l'ordinateur client.

Tableau 14-5. Emplacement des journaux View Client with Local Mode

Système d'exploitation	Chemin d'accès
Windows 8, Windows 7 et Windows Vista	`C:\Users\`*`user name`*`\AppData\Local\VMware\VDM\Logs\`
Windows XP	`C:\Documents and Settings\`*`nom d'utilisateur`*`\Local Settings\Application Data\VMware\VDM\Logs\`

Lorsqu'un poste de travail local est restitué ou répliqué, Serveur de transfert View transfère les données générées sur le poste de travail local depuis la dernière restitution ou réplication. Vous pouvez évaluer la taille potentielle du transfert de données si vous connaissez la durée nécessaire au le poste de travail pour créer les nouvelles données. L'exemple d'entrée de journal suivant indique la durée écoulée (en minutes) depuis la dernière restitution ou réplication :

```
2010-06-28 17:22:12,281 DEBUG <536> [wswc_localvm]
GetTotalCheckinSize: Total checkin size over 34 minutes:
```

Déterminer l'impact de la déduplication et de la compression

Les entrées de journal `GetTotalCheckinSize` indiquent la taille estimée du transfert avant son exécution. Ces chiffres englobent tous les disques du poste de travail local à partir duquel les données sont transférées.

L'exemple d'entrée suivant indique la quantité de données qui ne sera pas optimisée par la déduplication lors d'une opération de restitution. View évalue la quantité de données transférées.

```
2010-06-28 17:22:12,281 DEBUG <536> [wswc_localvm]
GetTotalCheckinSize: non-dedupe: 2 Mo
```

Dans les exemples d'entrées suivants, l'entrée `parent-dedupe` indique la quantité de données qui sera optimisée par la déduplication sur Serveur de transfert View. L'entrée `self-dedupe` indique la quantité de déduplication sur l'ordinateur client. Ajoutez les chiffres de ces entrées pour calculer la quantité totale de données qui sera optimisée par la déduplication.

```
2010-06-28 17:22:12,281 DEBUG <536> [wswc_localvm]
GetTotalCheckinSize: parent-dedupe: 871 Mo
2010-06-28 17:22:12,281 DEBUG <536> [wswc_localvm]
GetTotalCheckinSize: self-dedupe: 0 Mo
```

Les entrées de journal `Replication statistics` indiquent les quantités de données réelles envoyées sur le réseau. Des statistiques séparées sont générées pour chaque disque du poste de travail local à partir duquel les données sont transférées.

Dans l'exemple suivant, les entrées `parent-dedupe` et `self-dedupe` affichent des statistiques de déduplication sur Serveur de transfert View et sur l'ordinateur client, respectivement.

```
2010-06-28 17:24:53,046 DEBUG <BoraThread> [wswc_localvm]
Replication statistics:
2010-06-28 17:24:53,046 DEBUG <BoraThread> [wswc_localvm]
Parent dedup: 871.139 Mo
2010-06-28 17:24:53,046 DEBUG <BoraThread> [wswc_localvm]
Self dedup: 0.000 Mo
```

L'exemple d'entrée suivant indique la quantité de données compressée lors d'une opération de transfert :

```
2010-06-28 17:24:53,046 DEBUG <BoraThread> [wswc_localvm]
Compression: 0.000 Mo compressed to 0.000 Mo
```

L'exemple d'entrée suivant indique la quantité de données non compressée.

```
2010-06-28 17:24:53,046 DEBUG <BoraThread> [wswc_localvm] Raw
data: 2.198 Mo
```

Dans cet exemple, le poste de travail local affiche un message de type "`Transferring 871Mo`". Toutefois, cette quantité de données a été réduite par la déduplication. Bien que les données restantes n'aient pas pu être compressées, 2 198 Mo de données seulement ont été transférés sur le réseau.

Optimisation du système de fichiers client de transferts de données

Au cours l'opérations de transfert, Serveur de transfert View réduit la quantité de données devant être envoyées sur le réseau en bénéficiant de l'optimisation du système de fichiers client.

Lorsqu'une machine virtuelle de poste de travail contient une partition NTFS principale, Serveur de transfert View transfère les blocs alloués par NTFS. Les blocs non alloués ne sont pas transférés. Cette stratégie minimise le nombre total de blocs à transférer.

L'optimisation du système de fichiers client n'a lieu que lorsque des données sont transférées à partir de partitions NTFS principales. Serveur de transfert View n'effectue pas cette optimisation sur des partitions étendues, des partitions Gestionnaire de disque logique ou des volumes NTFS compressés sur des machines virtuelles Windows 8, Windows 7 ou Windows Vista.

L'optimisation du système de fichiers client est différente de la déduplication et de la compression des données, qui optimisent également les transferts de données mais qui sont indépendantes du système d'exploitation client du poste de travail. Pour plus d'informations sur ces opérations, reportez-vous à la section « Optimisation des transferts de données entre des ordinateurs hôte de poste de travail local et le datacenter », page 373.

Configuration de l'utilisation d'une ressource de point de terminaison

Par défaut, un poste de travail View emprunté pour une utilisation sur un système local bénéficie des capacités de mémoire et de CPU de cet hôte. Les cartes réseau virtuelles sur le poste de travail utilisent NAT pour partager les adresses IP et MAC de l'hôte. Vous pouvez modifier ce comportement par défaut.

Remplacer l'utilisation locale de mémoire et de ressources de CPU

Quand un poste de travail local est emprunté, il bénéficie des capacités de mémoire et de CPU du système local quels que soient les paramètres de mémoire et de CPU spécifiés pour la machine virtuelle dans vCenter Server. Vous pouvez remplacer ce comportement par défaut.

Par défaut, la quantité de RAM allouée à un poste de travail View emprunté pour une utilisation en mode local est automatiquement ajustée sur une certaine quantité de la RAM disponible sur l'hôte client.

La formule prend en compte la quantité de mémoire disponible pour être divisée entre les systèmes d'exploitation View hôte et client. Un système d'exploitation Windows XP requiert un minimum de 512 Mo de RAM. Un système d'exploitation Windows 8, Windows 7 ou Windows Vista 32 bits requiert un minimum de 1 Go de RAM. La quantité de mémoire disponible pour être divisée est la quantité totale de RAM sur l'hôte moins la RAM minimum requise pour les systèmes d'exploitation hôte et client.

Tableau 14-7. Mémoire allouée à des postes de travail View locaux

Allocation de mémoire	Clients Windows XP	Clients Windows 8, Windows 7 et Vista
Minimum	512 Mo	1 Go
Effort optimal	512 Mo + (Disponible/2)	1 Go + (Disponible/2)
Maximum	2 Go	4 Go

Par exemple, si un hôte Windows 7 a un total de 2 Go de RAM, l'exécution en local d'un poste de travail View Windows 7 nécessiterait 2 Go de RAM, avec 1 Go de RAM alloué à l'hôte et 1 Go de RAM alloué au poste de travail View local. Si l'hôte avait 3 Go de RAM, 1,5 Go de RAM serait alloué à l'hôte et 1,5 Go de RAM serait alloué au poste de travail View local.

Remarque L'ajustement automatique d'allocation de mémoire ne définit jamais la mémoire du poste de travail local sur une valeur inférieure à celle configurée dans vCenter Server.

De la même façon, le poste de travail View local peut utiliser jusqu'à deux CPU disponibles sur l'hôte client si le poste de travail View exécute un système d'exploitation Windows Vista ou supérieur.

Vous pouvez modifier les valeurs par défaut et spécifier la portée du paramètre. Le paramètre peut s'appliquer à tous les postes de travail locaux sur le client ou, en fonction du paramètre, il peut s'appliquer à un poste de travail spécifique ou à tous les postes de travail d'une instance de Serveur de connexion View spécifique qu'un utilisateur spécifique est autorisé à utiliser sur le client.

Pour modifier ces valeurs par défaut, vous devez configurer des paramètres de registre Windows. Vous pouvez alors utiliser des outils Windows standard tels que des Objets de stratégie de groupe (GPO) pour déployer ces paramètres de registre.

Prérequis

- Si vous prévoyez de définir un nombre spécifique de CPU pouvant être utilisés par le poste de travail local, mettez le poste de travail local hors tension.

- Comme dans de nombreux cas vous pouvez spécifier la portée du paramètre, déterminez les ID que vous devrez spécifier.

  Tableau 14-6. Identificateurs utilisés dans les paramètres de registre pour une utilisation des ressources en mode local

Portée	Nom de la variable	Description
Spécifique du serveur	*broker_guid*	Identificateur global unique (GUID) pour l'instance ou le groupe Serveur de connexion View. Utilisez la commande `vdmadmin -C` pour déterminer le GUID. Reportez-vous à la section « Définition du nom d'un groupe Serveur de connexion View à l'aide de l'option -C », page 470.
Spécifique du serveur et de l'utilisateur	*remote_user_sid*	ID de sécurité de l'utilisateur final. Utilisez l'utilitaire ADSI Edit sur un hôte de Serveur de connexion View et recherchez la valeur du champ **[pae-SIDString]** de **[CN=*machine_CN*,OU=Servers,DC=vdi,DC=vmware,DC=int]** .
Spécifique du serveur, de l'utilisateur et du poste de travail	*desktop_ID*	ID du poste de travail View. Utilisez l'utilitaire ADSI Edit sur un serveur Serveur de connexion View. L'ID est répertorié dans **[OU=Applications]** de **[DC=vdi,DC=vmware,DC=int]** . L'ID de poste de travail est le nom unique qui utilise le nom d'affichage du pool de postes de travail : **[CN=*pool_display_name*,OU=Applications,DC=vdi,DC=vmware,DC=int.]**

  Vous pouvez également rechercher le GUID du broker dans le fichier `mvdi.lst` sur l'ordinateur client. Sous Windows XP, le fichier se trouve dans le dossier `C:\Documents and Settings\`*`user_name`*`\Local Settings\Application Data\VMware\VDM`. Ouvrez le fichier et recherchez `brokerGUID`. L'ID de sécurité de l'utilisateur distant est également répertorié dans ce fichier. Ouvrez le fichier et recherchez `user-sid`.

Procédure

- Pour remplacer le comportement par défaut pour que le poste de travail local utilise la quantité de mémoire configurée dans vCenter Server, créez et déployez un GPO pour ajouter l'une des clés de registre suivantes et définissez la clé sur 1.

Portée du paramètre	Chemin d'accès
Client	`HKCU\Software\VMware, Inc.\VMware VDM\Client\disableOfflineDesktopMemoryScaleup`
Spécifique du serveur et de l'utilisateur	`HKCU\Software\VMware, Inc.\VMware VDM\Client\`*`broker_guid`*`\`*`remote_user_sid`*`\disableOfflineDesktopMemoryScaleup`

  La valeur 1 indique que `disableOfflineDesktopMemoryScaleup` est activé, et la valeur 0 indique qu'il est désactivé.

- Pour définir une quantité spécifique de mémoire pouvant être utilisée par le poste de travail View lors de son exécution en local, créez et déployez un GPO pour ajouter l'une des clés de registre suivantes spécifiant le nombre en mégaoctets, jusqu'à 32 Go.

Portée du paramètre	Chemin d'accès
Client	`HKCU\Software\VMware, Inc.\VMware VDM\Client\offlineDesktopDefaultMemoryScaleupValue`
Spécifique du serveur	`HKCU\Software\VMware, Inc.\VMware VDM\Client\`*`broker_guid`*`\offlineDesktopDefaultMemoryScaleupValue`
Spécifique du serveur et de l'utilisateur	`HKCU\Software\VMware, Inc.\VMware VDM\Client\`*`broker_guid`*`\`*`remote_user_sid`*`\offlineDesktopDefaultMemoryScaleupValue`
Spécifique du serveur, de l'utilisateur et du poste de travail	`HKCU\Software\VMware, Inc.\VMware VDM\Client\`*`broker_guid`*`\`*`remote_user_sid`*`\`*`desktop_ID`*`\offlineDesktopDefaultMemoryScaleupValue`

Si vous définissez la valeur sur un nombre trop important, le poste de travail local ne s'allume pas et un message d'erreur apparaît.

- Pour emprunter un poste de travail configuré pour nécessiter plus de mémoire qu'il n'en est disponible sur l'hôte client, créez et déployez un GPO pour ajouter la clé de registre suivante qui spécifie le nombre de mégaoctets signalés comme disponibles par le client local, comme vous l'avez défini.

  `HKCU\Software\VMware, Inc.\VMware VDM\Client\offlineDesktopReportedHostMemoryValue`

  Définir cette valeur sur une valeur supérieure ou égale à la mémoire requise par le poste de travail View vous permet d'emprunter et d'exécuter le poste de travail View si le client dispose de suffisamment de mémoire libre pour exécuter la machine virtuelle.

Portée du paramètre	Chemin d'accès
Client	`HKCU\Software\VMware, Inc.\VMware VDM\Client\offlineDesktopReportedHostMemoryValue`
Spécifique du serveur	`HKCU\Software\VMware, Inc.\VMware VDM\Client\`*`broker_guid`*`\offlineDesktopReportedHostMemoryValue`
Spécifique du serveur et de l'utilisateur	`HKCU\Software\VMware, Inc.\VMware VDM\Client\`*`broker_guid`*`\`*`remote_user_sid`*`\offlineDesktopReportedHostMemoryValue`
Spécifique du serveur, de l'utilisateur et du poste de travail	`HKCU\Software\VMware, Inc.\VMware VDM\Client\`*`broker_guid`*`\`*`remote_user_sid`*`\`*`desktop_ID`*`\offlineDesktopReportedHostMemoryValue`

  Si le client ne dispose pas de suffisamment de mémoire libre, vous pouvez utiliser le paramètre `offlineDesktopDefaultMemoryScaleupValue` avec le paramètre `offlineDesktopReportedHostMemoryValue`.

  Par exemple, si votre système client dispose de 2 Go de mémoire et si le poste de travail View est configuré pour nécessiter 2 Go de mémoire, vous ne pourrez pas emprunter le poste de travail View car de la mémoire est également requise pour la virtualisation hébergée par le client. Toutefois, vous pouvez utiliser le paramètre de registre `offlineDesktopReportedHostMemoryValue = 2048` pour pouvoir emprunter le poste de travail, et utiliser le paramètre de registre `offlineDesktopDefaultMemoryScaleupValue = 1024` pour que le poste de travail View utilise uniquement 1 Go de mémoire lorsqu'il est exécuté en local.

- Pour remplacer le comportement par défaut pour que le poste de travail local utilise le nombre de CPU configuré dans vCenter Server, créez et déployez un GPO pour ajouter l'une des clés de registre suivantes et définissez la clé sur 1.

Portée du paramètre	Chemin d'accès
Client	`HKCU\Software\VMware, Inc.\VMware VDM\Client\disableOfflineDesktopCPUScaleup`
Spécifique du serveur et de l'utilisateur	`HKCU\Software\VMware, Inc.\VMware VDM\Client\`*`broker_guid`*`\`*`remote_user_sid`*`\disableOfflineDesktopCPUScaleup`

  La valeur 1 indique que `disableOfflineDesktopCPUScaleup` est activé, et la valeur 0 indique qu'il est désactivé.

- Pour définir un nombre spécifique de CPU pouvant être utilisé par le poste de travail View lors de son exécution en local, créez et déployez un GPO pour ajouter l'une des clés de registre suivantes spécifiant le nombre de CPU, jusqu'à 2.

Portée du paramètre	Chemin d'accès
Client	HKCU\Software\VMware, Inc.\VMware VDM\Client\offlineDesktopDefaultCPUScaleupValue
Spécifique du serveur	HKCU\Software\VMware, Inc.\VMware VDM\Client*broker_guid*\offlineDesktopDefaultCPUScaleupValue
Spécifique du serveur et de l'utilisateur	HKCU\Software\VMware, Inc.\VMware VDM\Client*broker_guid**remote_user_sid*\offlineDesktopDefaultCPUScaleupValue
Spécifique du serveur, de l'utilisateur et du poste de travail	HKCU\Software\VMware, Inc.\VMware VDM\Client*broker_guid**remote_user_sid**desktop_ID*\offlineDesktopDefaultCPUScaleupValue

  Si vous spécifiez une valeur non valide, elle est ignorée et la valeur par défaut est utilisée. Si vous spécifiez un nombre de CPU supérieur au nombre de CPU disponibles sur l'hôte, le poste de travail local ne s'active pas et un message d'erreur apparaît. Si vous définissez la valeur sur un nombre supérieur à 2, la valeur 2 est utilisée.

Les paramètres prennent effet lorsque le poste de travail local est activé, sauf dans le cas où le paramètre autorisant que la mémoire requise signalée soit inférieure à celle définie sur vCenter Server est utilisé. Ce paramètre est en lecture seule lorsque le poste de travail est emprunté.

Passer le type de réseau de NAT à Relié par un pont

Par défaut, le type de réseau virtuel d'un poste de travail View passe à NAT (Network Address Translation) lorsque le poste de travail est emprunté pour être utilisé sur un système local. Vous pouvez remplacer ce comportement pour utiliser un réseau relié par un pont pour que le poste de travail View ait sa propre identité sur le réseau.

Avec le réseau relié par un pont, l'adaptateur réseau virtuel dans le poste de travail View se connecte à l'adaptateur réseau physique dans l'ordinateur hôte. Le réseau relié par un pont rend le poste de travail View visible pour les autres ordinateurs du réseau et requiert que le poste de travail ait sa propre adresse IP.

NAT configure une machine virtuelle pour partager les adresses IP et MAC de l'hôte. Le poste de travail View et l'hôte client partagent une seule identité réseau sur le réseau.

Pour modifier ces valeurs par défaut pour tous les postes de travail locaux ou pour des postes de travail locaux spécifiques sur un hôte client, vous devez configurer des paramètres de registre Windows. Vous pouvez alors utiliser des outils Windows standard tels que des Objets de stratégie de groupe (GPO) pour déployer ces paramètres de registre.

Prérequis

- Comme dans de nombreux cas vous pouvez spécifier la portée du paramètre, déterminez les ID que vous devrez spécifier.

  Tableau 14-8. Identificateurs utilisés dans les paramètres de registre pour une utilisation des ressources en mode local

Portée	Nom de la variable	Description
Spécifique du serveur	*broker_guid*	Identificateur global unique (GUID) pour l'instance ou le groupe Serveur de connexion View. Utilisez la commande `vdmadmin -C` pour déterminer le GUID. Reportez-vous à la section « Définition du nom d'un groupe Serveur de connexion View à l'aide de l'option -C », page 470.
Spécifique du serveur et de l'utilisateur	*remote_user_sid*	ID de sécurité de l'utilisateur final. Utilisez l'utilitaire ADSI Edit sur un hôte de Serveur de connexion View et recherchez la valeur du champ **[pae-SIDString]** de **[CN=*machine_CN*,OU=Servers,DC=vdi,DC=vmware,DC=int]** .
Spécifique du serveur, de l'utilisateur et du poste de travail	*desktop_ID*	ID du poste de travail View. Utilisez l'utilitaire ADSI Edit sur un serveur Serveur de connexion View. L'ID est répertorié dans **[OU=Applications]** de **[DC=vdi,DC=vmware,DC=int]** . L'ID de poste de travail est le nom unique qui utilise le nom d'affichage du pool de postes de travail : **[CN=*pool_display_name*,OU=Applications,DC=vdi,DC=vmware,DC=int.]**

  Vous pouvez également rechercher le GUID du broker dans le fichier `mvdi.lst` sur l'ordinateur client. Sous Windows XP, le fichier se trouve dans le dossier `C:\Documents and Settings\`*`user_name`*`\Local Settings\Application Data\VMware\VDM`. Ouvrez le fichier et recherchez `brokerGUID`. L'ID de sécurité de l'utilisateur distant est également répertorié dans ce fichier. Ouvrez le fichier et recherchez `user-sid`.

Procédure

- Pour remplacer le comportement par défaut pour que le poste de travail local utilise le réseau relié par un pont, créez et déployez un GPO pour ajouter l'une des clés de registre suivantes et définissez la clé sur 1.

Portée du paramètre	Chemin d'accès
Client	`HKCU\Software\VMware, Inc.\VMware VDM\Client\offlineDesktopUseBridgedNetworking`
Spécifique au serveur et à l'utilisateur	`HKCU\Software\VMware, Inc.\VMware VDM\Client\`*`broker_guid`*`\`*`remote_user_sid`*`\offlineDesktopUseBridgedNetworking`
Spécifique au serveur, à l'utilisateur et au poste de travail	`HKCU\Software\VMware, Inc.\VMware VDM\Client\`*`broker_guid`*`\`*`remote_user_sid`*`\`*`desktop_ID`*`\offlineDesktopUseBridgedNetworking`

  Une valeur de 1 définit le poste de travail pour qu'il utilise le réseau relié par un pont. Une valeur de 0 le définit pour qu'il utilise NAT, qui est la valeur par défaut.

Le paramètre prend effet lorsque l'utilisateur final met sous tension le poste de travail local.

Configuration d'un cache HTTP pour approvisionner des postes de travail locaux sur un réseau WAN

Vous pouvez utiliser un cache HTTP pour faciliter l'approvisionnement de postes de travail locaux de clone lié. La configuration d'un cache HTTP est avantageuse pour les bureaux distants et les succursales qui sont connectés au datacenter sur un réseau WAN. Le cache HTTP réduit les coûts de performance liés au transfert d'images de base de View Composer sur un réseau WAN.

Si vous configurez des postes de travail de clone lié pour utiliser le mode local dans des bureaux distants, votre réseau WAN peut ne pas disposer d'une bande passante suffisante pour télécharger efficacement l'image de base de View Composer directement sur chaque ordinateur local. Par exemple, le transfert répété d'une image de base de 6 Go peut être prohibitif.

Si vous configurez un cache HTTP, l'image de base est stockée dans le cache du serveur proxy lorsque le premier utilisateur emprunte le poste de travail. Quand d'autres utilisateurs empruntent des postes de travail, l'image de base est transférée sur le réseau LAN vers le bureau local.

Pour terminer une opération d'emprunt, View Transfer Server doit toujours transférer le disque du système d'exploitation et le disque persistant de clone lié de chaque utilisateur à partir du datacenter sur le réseau WAN, mais ces disques représentent une fraction de la taille de l'image de base.

1 Configurer Serveur de connexion View pour prendre en charge la mise en cache HTTP d'images de base de View Composer page 383

   Pour autoriser un serveur proxy de mise en cache à transmettre des images de base de View Composer et d'autres données entre des postes de travail locaux et le datacenter, vous devez configurer certains paramètres dans Serveur de connexion View.

2 Limiter la taille des fichiers de package d'image de base pour autoriser la mise en cache page 384

   Un package d'image de base View Composer peut contenir des fichiers dont la taille est supérieure à un gigaoctet, trop volumineuse pour qu'un certains nombre de serveurs proxy les mettent en cache. Vous pouvez configurer View Transfer Server pour diviser des packages d'image de base en fichiers dont la taille est inférieure à la capacité du cache du serveur proxy.

3 Configurer des ordinateurs client pour transférer des données via un serveur proxy page 385

   Pour prendre en charge la mise en cache HTTP, vous devez configurer les ordinateurs client qui hébergent des postes de travail locaux pour transférer les données de poste de travail via un serveur proxy de mise en cache. Vous devez également configurer les ordinateurs client pour utiliser l'adresse HTTP du serveur proxy pour des connexions Internet.

4 Configurer un serveur proxy pour mettre en cache des images de base de View Composer page 386

   Lorsque vous configurez un serveur proxy pour prendre en charge la mise en cache HTTP pour des postes de travail locaux, vous devez configurer la capacité du cache et la méthode de connexion HTTP.

Configurer Serveur de connexion View pour prendre en charge la mise en cache HTTP d'images de base de View Composer

Pour autoriser un serveur proxy de mise en cache à transmettre des images de base de View Composer et d'autres données entre des postes de travail locaux et le datacenter, vous devez configurer certains paramètres dans Serveur de connexion View.

Vous utilisez deux paramètres View séparés pour configurer le chiffrement SSL pour les deux types de données suivants :

- Images de base de View Composer
- Autres données de poste de travail de clone lié, y compris des disques de système d'exploitation et des disques persistants

Vous devez désactiver le chiffrement SSL de transferts de fichiers de package d'image de base depuis le référentiel de Serveur de transfert vers des ordinateurs locaux. La désactivation de SSL permet au serveur proxy d'accéder et de mettre en cache le contenu des fichiers de package. La désactivation de SSL n'expose pas les données d'image de base. Les données sont chiffrées lorsque vous publiez l'image de base sur le référentiel de Serveur de transfert et restent chiffrées lorsqu'elles sont téléchargées sur le serveur proxy sur le réseau WAN.

Vous pouvez choisir d'utiliser le chiffrement SSL de transferts de toutes les données de poste de travail local. Pour autoriser d'autres données de poste de travail local à passer via le serveur proxy de mise en cache, vous devez configurer le serveur proxy à autoriser l'utilisation de la méthode HTTP CONNECT ou vous devez activer le chiffrement SSL d'opérations de mode local sur Serveur de connexion View.

Si vous utilisez le chiffrement SSL, vous n'avez pas à modifier les paramètres de serveur proxy, mais le chiffrement SSL peut affecter les performances de transferts de disques du système d'exploitation et de disques persistants de clone lié.

Vous devez configurer ces paramètres SSL sur chaque instance de Serveur de connexion View qui fournit des services View aux clients pour lesquels vous configurez la mise en cache HTTP.

Procédure

1 Dans View Administrator, cliquez sur **[View Configuration (Configuration de View)] > [Servers (Serveurs)]** .

2 Cliquez sur l'onglet des serveurs Serveur de connexion View, sélectionnez une instance de Serveur de connexion View et cliquez sur **[Edit (Modifier)]** .

3 Cliquez sur l'onglet Local Mode (Mode local) et désélectionnez **[Use SSL when provisioning desktops in local mode (Utiliser SSL lors de l'approvisionnement de postes de travail en mode local)]** .

   Ce paramètre désactive SSL pour le téléchargement de fichiers de package d'image de base à partir du référentiel de Serveur de transfert vers les ordinateurs locaux.

4 Si vous ne définissez pas le serveur proxy de mise en cache pour utiliser la méthode HTTP CONNECT, sélectionnez **[Use SSL for Local Mode operations (Utiliser SSL pour des opérations en mode local)]** .

   Ce paramètre affecte les transferts de toutes les autres données de poste de travail local.

5 Cliquez sur **[OK]** .

Limiter la taille des fichiers de package d'image de base pour autoriser la mise en cache

Un package d'image de base View Composer peut contenir des fichiers dont la taille est supérieure à un gigaoctet, trop volumineuse pour qu'un certains nombre de serveurs proxy les mettent en cache. Vous pouvez configurer View Transfer Server pour diviser des packages d'image de base en fichiers dont la taille est inférieure à la capacité du cache du serveur proxy.

Lorsque vous publiez un package dans le référentiel de Transfer Server, View Transfer Server crée des fichiers de package de la taille spécifiée. Vous devez configurer la taille limite avant de commencer à publier des packages sur le référentiel. View Transfer Server ne divise pas les fichiers de package existants pour se conformer à la taille limite.

Vous pouvez définir cette valeur sur n'importe quelle instance de View Connection Server dans un groupe répliqué. Lorsque vous modifiez View LDAP, la modification est propagée à toutes les instances de View Connection Server répliquées.

Prérequis

Familiarisez-vous avec l'utilisation de la commande `vdmadmin` avec l'option –T. Reportez-vous à la section « Définition de la limite de division pour la publication de packages View Transfer Server à l'aide de l'option -T », page 492.

Procédure

1 Démarrez une invite de commande Windows sur votre ordinateur View Connection Server.

2 Saisissez la commande `vdmadmin` avec l'option `–T`.

```
vdmadmin –T [–packagelimit size_in_bytes]
```

Par défaut, le chemin d'accès vers le fichier exécutable de la commande `vdmadmin` est `C:\Program Files\VMware\VMware View\Server\tools\bin`.

Exemple : Définition de la taille limite du fichier de package

Définissez la limite de division du fichier de package sur 100 Mo.

```
vdmadmin –T –packagelimit 104857600
```

Affichez la limite de division du fichier de package actuelle.

```
vdmadmin –T
```

Configurer des ordinateurs client pour transférer des données via un serveur proxy

Pour prendre en charge la mise en cache HTTP, vous devez configurer les ordinateurs client qui hébergent des postes de travail locaux pour transférer les données de poste de travail via un serveur proxy de mise en cache. Vous devez également configurer les ordinateurs client pour utiliser l'adresse HTTP du serveur proxy pour des connexions Internet.

Pour autoriser des transferts à passer via un serveur proxy, vous ajoutez une clé de Registre aux ordinateurs client. Vous pouvez créer une stratégie de groupe dans Active Directory pour définir cette clé de Registre sur plusieurs ordinateurs dans un domaine.

Procédure

1 Démarrez l'éditeur de Registre Windows sur le système client de poste en mode local.

2 Dans le volet de gauche, développez le chemin du registre.

Processeur	Description
64 bits	`HKEY_LOCAL_MACHINE, SOFTWARE, Wow6432Node, VMware Inc., VMware VDM`
32 bits	`HKEY_LOCAL_MACHINE, SOFTWARE, VMware Inc., VMware VDM`

3 Cliquez sur **[Edit (Modifier)] > [New (Nouveau)] > [String Value (Valeur de chaîne)]** et saisissez **`useProxyForTransfer`** dans la nouvelle entrée de valeur.

4 Cliquez avec le bouton droit sur l'entrée **[useProxyForTransfer]** , cliquez sur **[Modify (Modifier)]** , saisissez **`true`** et cliquez sur **[OK]** .

L'entrée est ajoutée au Registre.

5 Quittez l'Éditeur du Registre Windows.

6 Sur l'ordinateur client, configurez les paramètres de connexion Internet Explorer pour utiliser votre serveur proxy de mise en cache.

a Démarrez Internet Explorer et cliquez sur **[Tools (Outils)] > [Internet Options (Options Internet)]** .

b Cliquez sur l'onglet **[Connections (Connexions)]** et cliquez sur **[LAN Settings (Paramètres réseau)]** .

c Cliquez sur **[Use a proxy server for your LAN (Utiliser un serveur proxy pour votre réseau local)]** et cliquez sur **[Advanced (Avancé)]** .

d Saisissez les adresses proxy et les numéros de port pour les connexions HTTP, Sécurisé, FTP et Socks et cliquez sur **[OK]** .

Configurer un serveur proxy pour mettre en cache des images de base de View Composer

Lorsque vous configurez un serveur proxy pour prendre en charge la mise en cache HTTP pour des postes de travail locaux, vous devez configurer la capacité du cache et la méthode de connexion HTTP.

Prérequis

- Vérifiez la taille limite de fichiers de package d'image de base que vous définissez avec la commande `vdmadmin -T`. Reportez-vous à la section « Limiter la taille des fichiers de package d'image de base pour autoriser la mise en cache », page 384.
- Déterminez si vous utilisez SSL pour des opérations en mode local. Reportez-vous à la section « Configurer Serveur de connexion View pour prendre en charge la mise en cache HTTP d'images de base de View Composer », page 383.

Procédure

1 Configurez la taille maximale du cache sur le serveur proxy.

Pour calculer la taille maximale, prenez en considération le nombre et la taille des images de base de View Composer qui sont utilisés par des postes de travail locaux. Les images de base sont téléchargées sous forme de fichiers de package vers le serveur proxy. Prenez aussi en considération d'autres fichiers que vous prévoyez de mettre en cache sur le serveur proxy.

2 Configurez la taille du fichier le plus volumineux pouvant être mis en cache.

La taille maximale d'un seul fichier sur le serveur proxy doit être au moins égale à la taille maximale du fichier de package que vous définissez avec la commande `vdmadmin -T`.

3 Si vous n'activez pas le paramètre **[Use SSL for Local Mode operations (Utiliser SSL pour des opérations en mode local)]** pour View Connection Server, définissez la liste de contrôle d'accès (ACL) sur le serveur proxy pour ouvrir le port 80 et autoriser la méthode CONNECT pour vous connecter au port 80.

View Transfer Server utilise la méthode CONNECT pour offrir une connexion par tunnel via le serveur proxy. View Transfer Server utilise cette connexion pour transférer des fichiers et des données autres que des images de base de View Composer entre des postes de travail locaux et le datacenter. L'utilisation du port 80 améliore les performances de transfert.

Configuration de l'intervalle de pulsation pour des ordinateurs client de poste de travail local

Les ordinateurs client qui hébergent des postes de travail locaux envoient des messages de pulsation à View Connection Server à des intervalles réguliers pour lire l'état de leurs postes de travail empruntés. L'intervalle de pulsation par défaut pour tous les ordinateurs client est de cinq minutes. Vous pouvez modifier l'intervalle de pulsation pour tous les ordinateurs client. Vous pouvez également définir un intervalle de pulsation différent pour un ordinateur client spécifique.

- Modifier l'intervalle de pulsation pour tous les ordinateurs client de poste de travail local page 387

  Pour modifier l'intervalle de pulsation de tous les ordinateurs client qui hébergent des postes de travail locaux, vous utilisez l'utilitaire ADSI Edit pour modifier View LDAP sur votre hôte de Serveur de connexion View. L'utilitaire ADSI Edit est installé avec Serveur de connexion View.

- Définir l'intervalle de pulsation pour un ordinateur client de poste de travail local spécifique page 387

  Pour définir l'intervalle de pulsation pour un ordinateur client spécifique qui héberge un poste de travail local, vous utilisez l'éditeur de Registre Windows pour modifier le registre système sur cet ordinateur.

Modifier l'intervalle de pulsation pour tous les ordinateurs client de poste de travail local

Pour modifier l'intervalle de pulsation de tous les ordinateurs client qui hébergent des postes de travail locaux, vous utilisez l'utilitaire ADSI Edit pour modifier View LDAP sur votre hôte de Serveur de connexion View. L'utilitaire ADSI Edit est installé avec Serveur de connexion View.

Lorsque vous modifiez View LDAP sur une instance de Serveur de connexion View, la modification est propagée à toutes les instances de Serveur de connexion View.

Prérequis

Pour plus d'informations sur l'utilisation de l'utilitaire ADSI Edit sur votre version du système d'exploitation Windows Server, consultez le site Web Microsoft TechNet.

Procédure

1. Démarrez l'utilitaire ADSI Edit sur votre hôte de Serveur de connexion View.
2. Dans la boîte de dialogue des paramètres de connexion, sélectionnez ou connectez-vous à **[DC=vdi, DC=vmware, DC=int]** .
3. Dans le volet Computer (Ordinateur), sélectionnez ou tapez **`localhost:389`** ou le nom de domaine complet qualifié (FQDN) de l'hôte de Serveur de connexion View suivi du port 389.

   Par exemple : **`localhost:389`** ou **`mycomputer.mydomain.com:389`**
4. Sur l'objet **[CN=Common, OU=Global, OU=Properties]** , définissez l'attribut **[pae-mVDIOfflineUpdateFrequency]** sur le nouvel intervalle de pulsation en minutes.

   Vous devez saisir un entier positif. Par défaut, cet attribut n'est pas défini. Lorsqu'il n'est pas défini, la valeur par défaut est de cinq minutes.

Le nouvel intervalle de pulsation prend effet la prochaine fois qu'un ordinateur client qui héberge un poste de travail local envoie un message de pulsation à Serveur de connexion View. Vous n'avez pas à redémarrer le service Serveur de connexion View ou l'ordinateur client.

Si l'intervalle de pulsation est défini sur une valeur inférieure sur un ordinateur client, View utilise la valeur de l'ordinateur client plutôt que la valeur de Serveur de connexion View. Par défaut, l'intervalle de pulsation n'est pas défini sur des ordinateurs client.

Définir l'intervalle de pulsation pour un ordinateur client de poste de travail local spécifique

Pour définir l'intervalle de pulsation pour un ordinateur client spécifique qui héberge un poste de travail local, vous utilisez l'éditeur de Registre Windows pour modifier le registre système sur cet ordinateur.

View n'utilise pas l'intervalle de pulsation défini sur l'ordinateur client si la valeur est supérieure à l'intervalle de pulsation défini sur l'hôte de Serveur de connexion View. View utilise toujours la plus petite des deux valeurs. L'intervalle de pulsation de Serveur de connexion View par défaut est de cinq minutes.

Prérequis

Pour plus d'informations sur l'utilisation de l'éditeur de Registre Windows sur la version du système d'exploitation Windows du système client en mode local, consultez le site Web Microsoft TechNet.

Procédure

1 Démarrez l'éditeur de Registre Windows sur l'ordinateur client de poste de travail local.

2 Ajoutez une nouvelle clé de Registre appelée **[policyUpdateFrequency]** .

L'emplacement du registre système dépend du type de processeur de l'ordinateur client.

Option	Action
64 bits	Ajoutez **[policyUpdateFrequency]** à `HKEY_LOCAL_MACHINE, SOFTWARE, Wow6432Node, VMware Inc., VMware VDM`.
32 bits	Ajoutez **[policyUpdateFrequency]** à `HKEY_LOCAL_MACHINE, SOFTWARE, VMware Inc., VMware VDM`.

3 Définissez la valeur de la clé **[policyUpdateFrequency]** sur le nouvel intervalle de pulsation en millisecondes.

Vous devez saisir un entier positif.

Téléchargement manuel d'un poste de travail local vers un emplacement avec de faibles connexions réseau

Pour les utilisateurs sur un réseau avec une bande passante extrêmement faible, l'emprunt d'un poste de travail peut être prohibitif car vous devez télécharger plusieurs gigaoctets de données. Pour servir ces utilisateurs, vous pouvez télécharger les fichiers de poste de travail manuellement et copiez les fichiers sur les ordinateurs client.

Par exemple, un utilisateur peut travailler chez lui dans un emplacement rural avec une connexion d'accès réseau à distance. L'utilisateur peut ne jamais se rendre dans le bureau principal, où le poste de travail peut être emprunté sur l'ordinateur de l'utilisateur sur le réseau LAN.

Dans ce cas, vous pouvez télécharger manuellement les fichiers de poste de travail vers un périphérique portable tel qu'un périphérique USB ou un DVD. Une fois que vous avez fourni le périphérique à l'utilisateur, ce dernier peut copier les fichiers dans un répertoire spécifié sur l'ordinateur client et emprunter le poste de travail depuis le datacenter View.

Vous ne pouvez utiliser cette approche qu'avec des postes de travail de clone lié View Composer.

- Vous téléchargez manuellement les fichiers d'image de base View Composer.
- Lorsque l'utilisateur emprunte le poste de travail, les fichiers de disque du système d'exploitation et de disque persistant de clone lié doivent toujours être téléchargés sur le réseau.

Toutefois, l'image de base contient les fichiers les plus volumineux. Par exemple, une image de base de Windows 8 ou Windows 7 peut contenir entre 6 et 10 Go. Le disque du système d'exploitation et le disque persistant représentent une fraction de cette taille.

1 Copier l'image de base à partir du référentiel de Serveur de transfert page 389

Pour télécharger un poste de travail manuellement vers un ordinateur client pour une utilisation en mode local, vous devez copier l'image de base de View Composer vers un périphérique portable. L'image de base est publiée en tant que package dans le référentiel de Serveur de transfert.

2 Copier les fichiers d'image de base sur l'ordinateur client page 389

Pour télécharger un poste de travail manuellement vers un ordinateur client pour une utilisation en mode local, vous devez copier les fichiers de package d'image de base à partir d'un périphérique portable sur l'ordinateur client.

3 Définir des autorisations pour permettre à View d'utiliser les fichiers de package copiés page 390

Pour que des opérations d'emprunt aient lieu pour le mode local, vous devez définir des autorisations sur les fichiers de package d'image de base qui ont été copiés dans le répertoire d'emprunt sur l'ordinateur client.

4 Emprunter un poste de travail après avoir copié manuellement l'image de base page 391

Une fois que vous avez copié manuellement l'image de base sur l'ordinateur client et défini des autorisations sur les fichiers de package, vous devez demander à l'utilisateur d'emprunter un poste de travail.

Copier l'image de base à partir du référentiel de Serveur de transfert

Pour télécharger un poste de travail manuellement vers un ordinateur client pour une utilisation en mode local, vous devez copier l'image de base de View Composer vers un périphérique portable. L'image de base est publiée en tant que package dans le référentiel de Serveur de transfert.

Prérequis

- Vérifiez que vous avez configuré View Manager pour déployer des postes de travail locaux. Reportez-vous à la section « Présentation de la configuration d'un déploiement de poste de travail local », page 351.
- Vérifiez que vous avez créé un pool de postes de travail de clone lié et publié un package sur le référentiel de Serveur de transfert. Reportez-vous à la section « Publier des fichiers de package dans le référentiel de Serveur de transfert », page 364.

Procédure

1 Dans View Administrator, cliquez sur **[View Configuration (Configuration de View)] > [Servers (Serveurs)]** .

2 Cliquez sur l'onglet des serveurs Serveur de transfert.

3 Dans le panneau du référentiel de Serveur de transfert, cliquez sur l'onglet Contents (Sommaire), sélectionnez le package associé au pool de postes de travail à partir duquel vous allez emprunter un poste de travail et cliquez sur **[Details (Détails)]** .

4 Vérifiez que le pool de postes de travail est associé à ce package.

5 Recherchez le chemin Repository (Référentiel), y compris l'ID de package.

Par exemple : `\\mycomputer.com\ImageRepository\Published\f222434a-e52a-4ce3-92d1-c14122fca996`

6 Copiez le contenu du package à partir du référentiel de Serveur de transfert sur le périphérique portable.

Vous devez copier l'intégralité du répertoire de package sur le périphérique portable.

Copier les fichiers d'image de base sur l'ordinateur client

Pour télécharger un poste de travail manuellement vers un ordinateur client pour une utilisation en mode local, vous devez copier les fichiers de package d'image de base à partir d'un périphérique portable sur l'ordinateur client.

Prérequis

- Vérifiez que l'utilisateur a installé View Client with Local Mode sur l'ordinateur client.
- Vérifiez que vous avez copié les fichiers de package sur un périphérique portable. Reportez-vous à la section « Copier l'image de base à partir du référentiel de Serveur de transfert », page 389.

Procédure

1 Fournissez à l'utilisateur le périphérique portable qui contient les fichiers de package du pool de postes de travail.

2 Copiez les fichiers de package sur un répertoire d'emprunt spécifié sur l'ordinateur client.

Copiez les fichiers vers un sous-répertoire dans le répertoire d'emprunt qui utilise le nom d'affichage du pool de postes de travail. Par exemple, pour télécharger des fichiers à partir d'un pool de postes de travail avec le nom d'affichage `LocalPool`, copiez les fichiers dans *`check_out_directory`*`\LocalPool`.

Répertoire d'emprunt	Description
Répertoire par défaut sur Windows 8, Windows 7 et Windows Vista	`C:\Users\`*`User Name`*`\AppData\Local\VMware\VDM\Local Desktops\`*`pool_display_name`*
Répertoire par défaut sur Windows XP	`C:\Documents and Settings\`*`User Name`*`\Local Settings\Application Data\VMware\VDM\Local Desktops\`*`pool_display_name`*
Répertoire personnalisé	Vous pouvez spécifier votre propre répertoire. Par exemple, pour télécharger des fichiers à partir d'un pool de postes de travail avec le nom d'affichage `LocalPool`, vous pouvez créer ce chemin : `C:\CheckOutDirectory\LocalPool`.

Définir des autorisations pour permettre à View d'utiliser les fichiers de package copiés

Pour que des opérations d'emprunt aient lieu pour le mode local, vous devez définir des autorisations sur les fichiers de package d'image de base qui ont été copiés dans le répertoire d'emprunt sur l'ordinateur client.

Vous devez supprimer l'attribut de lecture seule sur les fichiers de package et donner à l'utilisateur le privilège **Contrôle complet** sur le répertoire et tous les fichiers qu'il contient.

Cet exemple décrit comment définir des autorisations sur un ordinateur Windows 8 ou Windows 7. Sur les autres systèmes d'exploitation, les étapes sont un peu différentes.

Prérequis

Vérifiez que vous avez copié les fichiers de package dans un répertoire sur l'ordinateur client. Reportez-vous à la section « Copier les fichiers d'image de base sur l'ordinateur client », page 389.

Procédure

1 Ouvrez une session sur le système d'exploitation client Windows 8 ou Windows 7, cliquez sur l'icône **[Bibliothèques]** et allez dans le répertoire d'emprunt.

2 Cliquez avec le bouton droit sur le répertoire d'emprunt et cliquez sur **[Propriétés]** .

3 Cliquez sur l'onglet **[Sécurité]** et sur **[Modifier]** .

4 Dans la liste Noms de groupe ou d'utilisateur, sélectionnez le nom de l'utilisateur qui empruntera le poste de travail.

Si le nom d'utilisateur n'est pas dans la liste, cliquez sur **[Ajouter]** et ajoutez le nom d'utilisateur.

5 Cochez **[Contrôle complet]** dans la colonne **[Autoriser]** et cliquez sur **[OK]** .

6 Cliquez sur l'onglet **[Général]** et décochez **[Lecture seule (s'applique uniquement aux fichiers du dossier)]** .

Assurez-vous que la case est complètement décochée.

7 Dans la boîte de dialogue Confirmation des modifications d'attributs, assurez-vous que **[Appliquer les modifications à ce dossier, aux sous-dossiers et aux fichiers]** est sélectionné et cliquez sur **[OK]** .

Emprunter un poste de travail après avoir copié manuellement l'image de base

Une fois que vous avez copié manuellement l'image de base sur l'ordinateur client et défini des autorisations sur les fichiers de package, vous devez demander à l'utilisateur d'emprunter un poste de travail.

Prérequis

- Vérifiez que View Client with Local Mode est installé sur l'ordinateur client.
- Vérifiez que vous avez défini des autorisations pour utiliser des fichiers de package qui ont été copiés sur l'ordinateur client. Reportez-vous à la section « Définir des autorisations pour permettre à View d'utiliser les fichiers de package copiés », page 390.

Procédure

1. Sur l'ordinateur client, démarrez View Client, connectez-vous à Serveur de connexion View, ouvrez une session sur Serveur de connexion View et sélectionnez un pool de postes de travail.
2. Cliquez sur le bouton avec la flèche vers le bas à côté du pool de postes de travail et cliquez sur **[Emprunter]** .
3. (Facultatif) Si vous avez copié les fichiers de package vers un répertoire personnalisé, configurez View Client pour emprunter le poste de travail dans le répertoire personnalisé.
   a. Dans la boîte de dialogue Emprunter, cliquez sur **[Options]** .
   b. À côté du répertoire Emprunt, cliquez sur **[Parcourir]** et sélectionnez le répertoire qui contient le dossier de nom de pool.

      Ne sélectionnez pas le dossier de nom de pool lui-même.

      Par exemple, si vous avez copié les fichiers de package pour un pool avec un nom d'affichage `LocalPool` dans un répertoire nommé `C:\CheckOutDirectory\LocalPool`, sélectionnez le répertoire `C:\CheckOutDirectory`.
   c. Cliquez sur **[OK]** .
4. Dans la boîte de dialogue Emprunter, cliquez sur **[OK]** .

View Manager emprunte le poste de travail. Serveur de transfert View détecte que les fichiers d'image de base résident sur l'ordinateur client et ne télécharge que les fichiers de poste de travail restants. Ces fichiers incluent le disque du système d'exploitation et un disque persistant, si un tel disque est configuré.

Dépannage d'opérations de View Transfer Server et de poste de travail local

Des conseils de dépannage sont disponibles pour des opérations communes de View Transfer Server et de poste de travail local.

- Échec d'un emprunt avec l'erreur "Aucun Serveur de transfert disponible" page 393

  Lorsque les utilisateurs essaient d'emprunter des postes de travail, les opérations échouent et un message d'erreur `Aucun Serveur de transfert disponible` s'affiche.
- Problèmes avec les emprunts de poste de travail après l'emprunt initial page 394

  En supposant que View Transfer Server fonctionne correctement, vous pouvez penser que les problèmes d'emprunt sont dus au fait que View Connection Server ne possède plus la clé de chiffrement pour les fichiers sur la machine locale.
- La fenêtre d'ouverture de session prend un long moment pour s'afficher page 394

  Dans certaines circonstances, lorsque vous ouvrez View Client et spécifiez une instance de View Connection Server, la fenêtre d'ouverture de session ne s'affiche pas pendant 30 secondes minimum.

Échec d'un emprunt avec l'erreur "Aucun Serveur de transfert disponible"

Lorsque les utilisateurs essaient d'emprunter des postes de travail, les opérations échouent et un message d'erreur `Aucun Serveur de transfert disponible` s'affiche.

Problème

L'emprunt peut échouer lorsque l'opération est terminée à 10 %, avant que Serveur de transfert View démarre le transfert de données vers l'ordinateur client, mais l'opération peut également échouer plus tard au cours du processus. Par exemple, il est possible que l'image de base soit transférée vers l'ordinateur client, mais que les autres disques de la machine virtuelle ne puissent pas être transférés.

Ce problème se produit avec les opérations d'emprunt gérées par une instance Serveur de transfert View particulière.

Cause

Il peut également survenir suite à l'exécution de Serveur de transfert View sur un hôte ESX n'ayant pas accès aux magasins de données sur lesquels les postes de travail résident. Lors d'un emprunt, Serveur de transfert View transfère les données de poste de travail à partir des magasins de données sur l'ordinateur client. Les magasins de données doivent être accessibles depuis l'hôte ESX sur lequel la machine virtuelle Serveur de transfert View est exécutée.

Solution

- Migrez la machine virtuelle Serveur de transfert View vers un hôte ESX avec accès aux magasins de données.
  a. Dans View Administrator, placez l'instance de Serveur de transfert View en mode de maintenance.
  b. Dans vSphere Client, utilisez l'assistant Migration pour migrer la machine virtuelle Serveur de transfert View vers l'hôte ESX de destination.
  c. Dans View Administrator, sélectionnez l'instance de Serveur de transfert View et quittez le mode de maintenance.
- Si vous ne parvenez pas à migrer la machine virtuelle Serveur de transfert View, recréez Serveur de transfert View sur une autre machine virtuelle sur un hôte ESX avec accès aux magasins de données.
  a. Dans View Administrator, supprimez l'instance Serveur de transfert View de View Manager.
  b. Dans vSphere Client, désinstallez Serveur de transfert View ou supprimez la machine virtuelle Serveur de transfert View.
  c. Créez une machine virtuelle sur l'hôte ESX de destination.
  d. Installez Serveur de transfert View sur la machine virtuelle.
  e. Dans View Administrator, ajoutez Serveur de transfert View à View Manager.

  Pour plus d'informations sur l'installation de Serveur de transfert View, consultez le document *Installation de VMware Horizon View*.

Problèmes avec les emprunts de poste de travail après l'emprunt initial

En supposant que View Transfer Server fonctionne correctement, vous pouvez penser que les problèmes d'emprunt sont dus au fait que View Connection Server ne possède plus la clé de chiffrement pour les fichiers sur la machine locale.

Problème

Après avoir réussi à emprunter un poste de travail local et à le restituer, vous empruntez de nouveau le poste de travail, mais vous ne pouvez pas vous connecter au poste de travail local. Vous pouvez voir un message d'erreur tel que `Cannot access local desktop--desktop corrupted`.

Cause

Si vous modifiez le cryptage de clé de chiffrement pour un poste de travail local, ou si vous supprimez le poste de travail depuis son pool et que vous en créez un nouveau, View Connection Server utilise une nouvelle clé d'authentification pour générer un nouveau fichier de configuration.

Lorsque des utilisateurs finaux essaient d'emprunter de nouveau le poste de travail, seuls les fichiers modifiés sont téléchargés. Les nouveaux fichiers qui sont téléchargés utilisent une nouvelle clé de chiffrement, mais les anciens fichiers déjà sur la machine locale utilisent l'ancienne clé de chiffrement, que View Connection Server ne possède plus.

Solution

- Les utilisateurs finaux doivent supprimer tous les fichiers de poste de travail local avant d'emprunter de nouveau le poste de travail.

  Le dossier réside dans le répertoire d'emprunt du poste de travail local. Lors du téléchargement de votre premier poste de travail local, si vous n'avez pas cliqué sur **[Options]** et modifier le répertoire de stockage des postes de travail locaux, ces derniers sont stockés dans le répertoire d'emprunt défini par défaut.

Système d'exploitation du poste de travail	Répertoire d'emprunt par défaut
Répertoire par défaut sur Windows 8, Windows 7 et Windows Vista	`C:\Users\`*`User Name`*`\AppData\Local\VMware\VDM\Local Desktops\`*`pool_display_name`*
Répertoire par défaut sur Windows XP	`C:\Documents and Settings\`*`User Name`*`\Local Settings\Application Data\VMware\VDM\Local Desktops\`*`pool_display_name`*

La fenêtre d'ouverture de session prend un long moment pour s'afficher

Dans certaines circonstances, lorsque vous ouvrez View Client et spécifiez une instance de View Connection Server, la fenêtre d'ouverture de session ne s'affiche pas pendant 30 secondes minimum.

Problème

Parfois, la fenêtre d'ouverture de session n'est pas accessible pendant une trentaine de secondes, jusqu'à l'expiration de la tentative de connexion.

Cause

Si View Client utilise une adresse IP pour View Connection Server, ce problème survient si vous disposez d'une connexion réseau mais que View Connection Server est inaccessible. Ce problème peut par exemple se produire si vous tentez d'ouvrir une session sur un poste de travail local depuis votre domicile, lorsque vous disposez d'une connexion Internet mais pas d'une connexion VPN qui permettrait d'accéder à View Connection Server.

Si View Client utilise un nom d'hôte plutôt qu'une adresse IP, sur un réseau local, ce problème signifie que View Connection Server, ou un proxy le cas échéant, est en panne ou qu'un pare-feu bloque la connexion. Sur un réseau WAN (Wide-Area Network), ce problème peut avoir la même origine ou peut signifier que le nom d'hôte est résolvable sur DNS public mais que le serveur n'est pas conçu pour être accessible depuis le réseau WAN.

Solution

Vous devez attendre l'expiration de la tentative de connexion. La fenêtre d'ouverture de session finit par s'afficher.

Serveur de transfert View reste dans un état En attente

Serveur de transfert View n'est pas disponible tant qu'il reste dans un état En attente pendant une période assez longue. Par exemple, l'état d'attente peut durer plus de dix minutes.

Problème

Quand vous avez ajouté Serveur de transfert View à View Manager, l'état de Serveur de transfert View ne passe pas sur Prêt.

Cause

Une cause commune est que Serveur de connexion Viewne peut pas se connecter à Serveur de transfert View.

Solution

- Vérifiez que Serveur de transfert View est installé sur la machine virtuelle.
- Vérifiez que les services Serveur de transfert View sont en cours d'exécution.
  a Sur la machine virtuelle Serveur de transfert View, ouvrez la boîte de dialogue **[Panneau de configuration] > [Outils d'administration] > [Services]** .
  b Vérifiez que les services VMware Serveur de transfert View, Serveur de transfert View Control et VMware View Framework Component sont démarrés.
- Vérifiez que la machine virtuelle Serveur de transfert View peut résoudre le nom de l'hôte Serveur de connexion View.
- Vérifiez que la machine Serveur de connexion View peut effectuer un test ping sur l'adresse IP de Serveur de transfert View.
- Vérifiez que la machine virtuelle Serveur de transfert View satisfait la configuration système recommandée. Consultez la configuration requise de Serveur de transfert View dans le document *Installation de VMware Horizon View*.

View Transfer Server ne peut pas passer en mode de maintenance

Lorsque vous tentez de placer View Transfer Server en mode de maintenance, il reste en état d'attente du mode de maintenance pendant une période assez longue.

Problème

Lorsque View Transfer Server est en état d'attente du mode de maintenance, vous ne pouvez pas effectuer des opérations telles que la migration du référentiel de Transfer Server vers un nouvel emplacement, que vous pouvez faire une fois que View Transfer Server passe en mode de maintenance.

Cause

Les opérations de transfert actif ou de publication de package vers le référentiel de Transfer Server sont toujours en cours.

Solution

Attendez que les transferts de données actifs et les opérations de publication soient terminés. Lorsque toutes les opérations sont terminées, View Transfer Server passe en mode de maintenance.

Le référentiel de Transfer Server est non valide

Dans View Administrator, View Transfer Server affiche l'état Bad Transfer Server repository (Mauvais référentiel de Transfer Server).

Problème

Vous ne pouvez pas effectuer des opérations de transfert pour des postes de travail de clone lié ou publier des packages tant que View Transfer Server est dans cet état.

Cause

Le référentiel de Transfer Server auquel View Transfer Server doit se connecter est différent du référentiel de Transfer Server actuellement configuré dans View Connection Server.

Une migration non valide du référentiel de Transfer Server peut entraîner le passage de View Transfer Server dans cet état.

Solution

Migrez de nouveau le référentiel de Transfer Server vers un nouvel emplacement. Pour plus d'informations, reportez-vous à la section « Migrer le référentiel de Serveur de transfert vers un nouvel emplacement », page 365.

Serveur de transfert View ne peut pas se connecter au référentiel de Serveur de transfert

Dans View Administrator, Serveur de transfert View affiche l'état Repository Connection Error (Erreur de connexion au référentiel).

Problème

Serveur de transfert View ne peut pas se connecter au référentiel de Serveur de transfert qui est configuré dans Serveur de connexion View.

Cause

La configuration du référentiel de Serveur de transfert est non valide. Si le référentiel est configuré sur un partage de réseau, le chemin de réseau ou les informations d'identification sont invalides. Si le référentiel est local, le chemin d'accès au système de fichiers est invalide.

Solution

1 Placez toutes les instances de Serveur de transfert View en mode de maintenance.

   a Dans View Administrator, cliquez sur **[View Configuration (Configuration de View)] > [Servers (Serveurs)]** .

   b Cliquez sur l'onglet des serveurs Serveur de transfert et sélectionnez une instance de Serveur de transfert View.

   c Cliquez sur **[Enter Maintenance Mode (Passer en mode de maintenance)]** .

   d Si des transferts sont actuellement actifs, choisissez d'annuler les transferts actifs ou attendez que les transferts actifs soient terminés avant de passer l'instance de Serveur de transfert View en mode de maintenance.

e Cliquez sur **[OK]** .

f Répétez ces étapes pour toutes les instances Serveur de transfert View.

2 Dans le panneau du référentiel de Serveur de transfert, cliquez sur l'onglet General (Général).

3 Cliquez sur **[Edit (Modifier)]** et configurez de nouveau le référentiel de Serveur de transfert.

Serveur de transfert View vérifie que le référentiel de Serveur de transfert est valide.

Serveur de transfert View ne peut pas vérifier l'intégrité

Dans View Administrator, Serveur de transfert View affiche l'état Mauvaise vérification d'intégrité. Le tableau de bord de View Administrator affiche Serveur de transfert View avec une flèche vers le bas rouge.

Problème

Dans un état Mauvaise vérification d'intégrité, Serveur de transfert View ne peut fonctionner correctement. Vous ne pouvez pas effectuer des opérations de transfert ou publier des packages dans le référentiel de Serveur de transfert.

Cause

Serveur de transfert View n'est pas disponible, n'est pas en cours d'exécution ou ne fonctionne pas correctement.

Solution

- Vérifiez que Serveur de transfert View est installé sur la machine virtuelle.
- Vérifiez que les services Serveur de transfert View sont en cours d'exécution.
  a Sur la machine virtuelle Serveur de transfert View, ouvrez la boîte de dialogue **[Panneau de configuration] > [Outils d'administration] > [Services]** .
  b Vérifiez que les services VMware Serveur de transfert View, Serveur de transfert View Control et VMware View Framework Component sont démarrés.
- Vérifiez que la machine virtuelle Serveur de transfert View peut résoudre le nom de l'hôte Serveur de connexion View.
- Vérifiez que la machine Serveur de connexion View peut effectuer un test ping sur l'adresse IP de Serveur de transfert View.
- Vérifiez que la machine virtuelle Serveur de transfert View satisfait la configuration système recommandée. Consultez la configuration requise de Serveur de transfert View dans le *Guide d'installation de VMware Horizon View*.

référentiel de Serveur de transfert n'est pas configuré

Dans View Administrator, Serveur de transfert View affiche l'état No Serveur de transfert Repository Configured (Aucun référentiel de Serveur de transfert configuré).

Problème

Vous ne pouvez pas effectuer des opérations de transfert pour des postes de travail de clone lié ou publier des packages dans le référentiel de Serveur de transfert.

Cause

Le référentiel de Serveur de transfert n'est pas configuré dans View Manager.

Solution

1 Placez toutes les instances de Serveur de transfert View en mode de maintenance.

   a Dans View Administrator, cliquez sur **[View Configuration (Configuration de View)] > [Servers (Serveurs)]** .

   b Cliquez sur l'onglet des serveurs Serveur de transfert et sélectionnez une instance de Serveur de transfert View.

   c Cliquez sur **[Enter Maintenance Mode (Passer en mode de maintenance)]** .

   d Si des transferts sont actuellement actifs, choisissez d'annuler les transferts actifs ou attendez que les transferts actifs soient terminés avant de passer l'instance de Serveur de transfert View en mode de maintenance.

   e Cliquez sur **[OK]** .

   f Répétez ces étapes pour toutes les instances Serveur de transfert View.

2 Dans le panneau du référentiel de Serveur de transfert, cliquez sur l'onglet General (Général).

3 Cliquez sur **[Edit (Modifier)]** et configurez le référentiel de Serveur de transfert.

   Serveur de transfert View vérifie que le référentiel de Serveur de transfert est valide.

Des instances de View Transfer Server ont des référentiels de Transfer Server en conflit

Dans View Administrator, des intances de View Transfer Server affichent l'état Transfer Server Repository Conflict (Conflit de référentiel de Transfer Server).

Problème

Vous ne pouvez pas effectuer des opérations de transfert pour des postes de travail de clone lié ou publier des packages dans le référentiel de Transfer Server.

Cause

Plusieurs instances de View Transfer Server sont configurées pour se connecter à différents référentiels de Transfer Server.

Cet état se produit si plusieurs instances de View Transfer Server sont simultanément ajoutées à View Manager, et que chaque instance est configurée avec un référentiel de Transfer Server différent.

Solution

Supprimez les instances de View Transfer Server de View Manager et ajoutez-les une par une. Si une instance de View Transfer Server affiche l'état Bad Transfer Server Repository (Mauvais référentiel de Transfer Server), reportez-vous aux informations de dépannage dans la section « Le référentiel de Transfer Server est non valide », page 396.

Le service Web de View Transfer Server est arrêté

Dans View Administrator, View Transfer Server affiche l'état Web Server Down (Serveur Web arrêté).

Problème

View Transfer Server ne peut pas télécharger des packages depuis le référentiel de Transfer Server, ni transférer d'autres données de poste de travail sur des postes de travail locaux.

Cause

Le service Web Apache2.2 qui prend en charge le référentiel de Transfer Server n'est pas en cours d'exécution.

Solution

1 Sur la machine virtuelle View Transfer Server, ouvrez la boîte de dialogue **[Control Panel (Panneau de configuration)] > [Administrative Tools (Outils d'administration)] > [Services]** .

2 Démarrez le service Apache2.2.

Une opération en mode local échoue après modification du poste de travail du datacenter

Au cours d'une opération en mode local, telle qu'un emprunt ou une restitution, l'opération échoue avec le message suivant affiché : `This desktop has been modified at the datacenter. Please contact your system administrator (Ce poste de travail a été modifié dans le datacenter. Contactez l'administrateur système.)`.

Problème

Une opération en mode local échoue lorsqu'un utilisateur démarre une opération ou que l'opération est interrompue ou suspendue, puis reprend. Ce problème peut apparaître avec les opérations suivantes en mode local : emprunt, reprise d'emprunt, annulation d'emprunt, restitution, reprise de restitution, annulation de restitution, restauration, lancement de réplication, reprise de réplication.

Outre le message d'erreur utilisateur, des événements View sont générés si la base de données des événements View est configurée et que des messages sont générés dans les journaux de Serveur de connexion View.

Si le problème apparaît lors d'une réplication, l'état de l'opération devient `Wait to resume backup (Attendre pour reprendre la sauvegarde)`. Le message d'erreur `This desktop has been modified at the datacenter. Please contact your system administrator (Ce poste de travail a été modifié dans le datacenter. Contactez l'administrateur système).` ne s'affiche pas à l'attention de l'utilisateur.

Cause

Lorsqu'un poste de travail View est emprunté, un snapshot est créé dans vCenter Server afin de préserver l'état de la machine virtuelle. La version vCenter Server du poste de travail est verrouillée pour qu'aucun autre utilisateur ne puisse y accéder.

Ce problème peut apparaître si vSphere permet de déverrouiller la copie du datacenter d'une machine virtuelle et qu'un autre processus ou une autre personne active la machine virtuelle par erreur. Par exemple, une machine virtuelle peut être déverrouillée pendant une mise à niveau vCenter Server. La machine virtuelle dans le datacenter et le poste de travail local ne sont plus synchronisés.

Lorsqu'une opération en mode local est démarrée ou reprise, View détecte que les versions de machine virtuelle ne sont pas synchronisées et arrête l'opération.

Solution

Vous pouvez récupérer la version client ou la version de vCenter Server de la machine virtuelle en fonction de l'opération en mode local qui était en cours.

Si une restitution ou une réplication a échoué, récupérez la version client. Vous pouvez utiliser une commande `vdmadmin –V` qui ramène la machine virtuelle vCenter Server au snapshot qui a été pris au cours de la dernière synchronization.

1 Sur l'ordinateur Serveur de connexion View, ouvrez une invite de commande et accédez au répertoire `C:\Program Files\VMware\VMware View\Server\tools\bin`.

2 Exécutez la commande `vdmadmin –V –recoverClientVM`.

Par exemple : `vdmadmin –V –recoverClientVM –d lmdtpool –m machine1`

3 Demandez à l'utilisateur de redémarrer l'opération de restitution.

Si un emprunt a échoué, récupérez la version vCenter Server. Vous pouvez utiliser une commande `vdmadmin -V` qui crée un nouveau snapshot de la machine virtuelle vCenter Server, supprime l'ancien snapshot et restaure la machine virtuelle. Au cours d'une restauration, le poste de travail local View est supprimé.

1 Sur l'ordinateur Serveur de connexion View, ouvrez une invite de commande et accédez au répertoire `C:\Program Files\VMware\VMware View\Server\tools\bin`.

2 Exécutez la commande `vdmadmin -V -recoverServerVM`.

Par exemple : `vdmadmin -V -recoverServerVM -d lmdtpool -m machine2`

3 Demandez à l'utilisateur de redémarrer l'opération d'emprunt.

Dans une situation particulière dans laquelle un poste de travail est complètement emprunté et aucune restitution ou réplication n'était en cours lorsque la machine virtuelle vCenter Server a été ouverte, vous pouvez conserver les machines virtuelles clientes et vCenter Server. Il se peut que du contenu utile valide ait été créé sur les deux machines virtuelles. Dans vCenter Server, vous pouvez cloner la machine virtuelle vCenter Server pour conserver une copie identique. Ensuite, vous pouvez utiliser la commande `vdmadmin` avec l'option `-V -recoverClientVM` pour récupérer la machine virtuelle cliente.

Pour plus d'informations sur l'utilisation de la commande `vdmadmin` avec l'option `-V`, voir « Récupération d'un poste de travail en utilisant l'option -V lorsque le poste de travail a été modifié dans le datacenter », page 494.

Restaurer des données à partir d'un poste de travail local

Présentation sécurise la machine virtuelle d'un poste de travail local en cryptant tous ses disques virtuels. Si l'identifiant d'emprunt de la machine virtuelle est supprimé de la configuration, ou si les fichiers de la session ou des règles sont corrompus, vous ne pourrez peut-être pas alimenter ou restituer la poste de travail local. Vous pouvez décrypter la machine virtuelle du poste de travail de façon à en restaurer certaines données.

IMPORTANT N'utilisez cette procédure que si aucune autre méthode ne vous permet de restaurer les données dans le poste de travail.

L'instance de Serveur de connexion View doit avoir accès à la configuration View LDAP contenant la clé d'authentification du poste de travail local.

En fonction du volume de données à restaurer, vous pouvez choisir de décrypter la machine virtuelle complète ou l'un de ses disques. Le processus de décryptage est plus rapide si vous décryptez un seul disque.

Prérequis

- Vérifiez que vous ne pouvez pas restaurer le poste de travail sans perte de données.
- Vérifiez que les données du poste de travail local n'ont pas été répliquées ou enregistrées à un autre emplacement.
- Connectez-vous en tant qu'utilisateur dans le rôle **Administrateurs** sur l'ordinateur Windows sur lequel l'instance de Serveur de connexion View est installée.
- Assurez-vous que le dossier dans lequel vous souhaitez effectuer le décryptage dispose d'un espace suffisant pour stocker les fichiers de la machine virtuelle cryptée et de la machine virtuelle décryptée. Vérifiez également que vous avez un droit d'écriture sur le dossier.

Procédure

1 À partir de la machine client, copiez les fichiers de la machine virtuelle dans un dossier local sur l'instance de Serveur de connexion View.

IMPORTANT N'utilisez pas un partage de réseau ni un lecteur mappé pour accéder aux fichiers.

2 Pour décrypter un fichier, exécutez la commande `vdmadmin`.

```
vdmadmin –V –rescue –d desktop –u domain\user –infile path_to_VM_file
```

Option	Description
–d *poste de travail*	Spécifie le nom du pool de postes de travail.
–infile *path_to_VM_file*	Spécifie le chemin d'accès au fichier de machine virtuelle pour la machine virtuelle du poste de travail. Pour restaurer une machine virtuelle complète, spécifiez le nom du fichier de configuration de la machine virtuelle VMware (fichier VMX) comme argument de l'option `–infile`. Pour restaurer un seul disque d'une machine virtuelle, spécifiez le nom du fichier de disque virtuel VMware (fichier VMDK) comme argument de l'option `–infile`. Ne sélectionnez pas un fichier VMDK correspondant à une partition de disque.
–u *domain\user*	Spécifie le domaine et le nom de l'utilisateur final du poste de travail local.

La commande `vdmadmin` écrit les fichiers de la machine virtuelle décryptée dans un sous-dossier nommé `rescued`.

Exemple : Décrypter des fichiers de machine virtuelle

Décryptez une machine virtuelle complète en sélectionnant son fichier VMX.

```
vdmadmin –V –rescue –d lmdtpool –u MYCORP\jo –infile
"J:\Temp\LMDT_Recovery\CN=lmdtpool,OU=Applications,DC=mycorp,DC=com.vmx"
```

Répertoriez les fichiers disponibles pour le disque `scsi00` de la machine virtuelle d'un poste de travail local.

```
J:\Temp\LMDT_Recovery>dir /b *scsi00*
52e52b7c26a2f683–42b945f934e0fbb2–scsi00–000001.vmdk
52e52b7c26a2f683–42b945f934e0fbb2–scsi00–000001–s001.vmdk
52e52b7c26a2f683–42b945f934e0fbb2–scsi00–000001–s002.vmdk
52e52b7c26a2f683–42b945f934e0fbb2–scsi00–000001–s003.vmdk
52e52b7c26a2f683–42b945f934e0fbb2–scsi00–000001–s004.vmdk
5215df4df635a14d–caf14c8dbbb14a3d–scsi00.vmdk
5215df4df635a14d–caf14c8dbbb14a3d–scsi00–s001.vmdk
5215df4df635a14d–caf14c8dbbb14a3d–scsi00–s002.vmdk
5215df4df635a14d–caf14c8dbbb14a3d–scsi00–s003.vmdk
5215df4df635a14d–caf14c8dbbb14a3d–scsi00–s004.vmdk
```

Décryptez la version actuelle du disque `scsi00` en sélectionnant son fichier VMDK.

```
vdmadmin –V –rescue –d lmdtpool –u MYCORP\jo –infile
"J:\Temp\LMDT_Recovery\52e52b7c26a2f683–42b945f934e0fbb2–scsi00–000001.vmdk"
```

Suivant

Utilisez VMware Workstation pour alimenter et examiner une machine virtuelle complète décryptée, ou VMware DiskMount pour monter un disque décrypté. Vous pouvez aussi examiner le contenu d'un disque décrypté en attachant son fichier VMDK à une machine virtuelle dans VMware Workstation. Après avoir restauré les données à partir de fichiers de la machine virtuelle, restaurez le poste de travail local.

Maintenance des composants View 15

Pour garder vos composants View disponibles et exécutés, vous pouvez effectuer diverses tâches de maintenance.

Ce chapitre aborde les rubriques suivantes :

Sauvegarde et restauration de données de configuration de View

Vous pouvez sauvegarder vos données de configuration de View Manager et View Composer en planifiant ou en exécutant des sauvegardes automatiques dans View Administrator. Vous pouvez restaurer votre configuration de View en important manuellement les fichiers View LDAP sauvegardés et les fichiers de base de données View Composer.

Vous pouvez utiliser les fonctions de sauvegarde et de restauration pour conserver et migrer des données de configuration de View.

Sauvegarde des données de Serveur de connexion View et de View Composer

Après avoir terminé la configuration initiale de Serveur de connexion View, vous pouvez planifier des sauvegardes régulières de vos données de configuration de View Manager et de View Composer. Vous pouvez conserver vos données View Manager et View Composer en utilisant View Administrator.

View Manager stocke des données de configuration de Serveur de connexion View dans le référentiel View LDAP. View Composer stocke des données de configuration pour des postes de travail de clone lié dans la base de données View Composer.

Lorsque vous utilisez View Administrator pour effectuer des sauvegardes, View Manager sauvegarde les données de configuration View LDAP et la base de données View Composer. Les deux jeux de fichiers de sauvegarde sont stockés dans le même emplacement. Les données de View LDAP sont exportées au format LDIF (LDAP Data Interchange Format) crypté. Pour voir une description de View LDAP, reportez-vous à la section « Répertoire View LDAP », page 39.

Vous pouvez effectuer les sauvegardes de plusieurs façons.

- Planifiez des sauvegardes automatiques en utilisant la fonction Sauvegarde de configuration de View Manager.
- Initiez une sauvegarde immédiatement en utilisant la fonction **[Sauvegarder maintenant]** dans View Administrator.
- Exportez manuellement des données View LDAP en utilisant l'utilitaire `vdmexport`. Cet utilitaire est fourni avec chaque instance de Serveur de connexion View.

  L'utilitaire `vdmexport` peut exporter des données View LDAP sous forme de données LDIF cryptées, de texte brut ou de texte brut avec des mots de passe et autres données sensibles supprimés.

  Remarque L'outil `vdmexport` sauvegarde uniquement les données View LDAP. Cet outil ne sauvegarde pas les informations sur la base de données View Composer.

  Pour plus d'informations sur `vdmexport`, reportez-vous à la section « Exporter des données de configuration depuis Serveur de connexion View », page 405.

Les recommandations suivantes s'appliquent à la sauvegarde des données de configuration View :

- View Manager peut exporter des données de configuration depuis n'importe quelle instance de Serveur de connexion View.
- Si vous possédez plusieurs instances de Serveur de connexion View dans un groupe répliqué, vous devez uniquement exporter les données depuis une seule instance. Toutes les instances répliquées contiennent les mêmes données de configuration.
- Ne vous attendez pas ce que des instances répliquées de Serveur de connexion View agissent comme votre mécanisme de sauvegarde. Lorsque View Manager synchronise des données dans des instances répliquées de Serveur de connexion View, toutes les données perdues dans une instance peuvent être perdues dans tous les membres du groupe.
- Si Serveur de connexion View utilise plusieurs instances de vCenter Server avec plusieurs services View Composer, View Manager sauvegarde toutes les bases de données View Composer associées aux instances de vCenter Server.

Planifier des sauvegardes de configuration de View Manager

Vous pouvez planifier la sauvegarde de vos données de configuration de View Manager à des intervalles réguliers. View Manager sauvegarde le contenu du référentiel View LDAP dans lequel vos instances de Serveur de connexion View stockent leurs données de configuration.

Vous pouvez sauvegarder la configuration immédiatement en sélectionnant l'instance de Serveur de connexion View et en cliquant sur **[Sauvegarder maintenant]** .

Prérequis

Familiarisez-vous avec les paramètres de sauvegarde. Reportez-vous à la section « Paramètres de sauvegarde de configuration de View Manager », page 405.

Procédure

1 Dans View Administrator, cliquez sur **[Configuration]** > **[Serveurs]** .

2 Sélectionnez l'instance de Serveur de connexion View à sauvegarder et cliquez sur **[Modifier]** .

3 Cliquez sur l'onglet Sauvegarde.

4 Spécifiez les paramètres de Sauvegarde de configuration de View Manager pour configurer la fréquence de sauvegarde, le nombre maximum de sauvegardes et l'emplacement du dossier des fichiers de sauvegarde.

5 (Facultatif) Modifiez le mot de passe de récupération de données.

   a Cliquez sur **[Modifier le mot de passe de récupération de données]** .

   b Tapez et retapez le nouveau mot de passe.

   c (Facultatif) Tapez un rappel de mot de passe.

   d Cliquez sur **[OK]** .

6 Cliquez sur **[OK]** .

Paramètres de sauvegarde de configuration de View Manager

View Manager peut sauvegarder vos données de configuration de Serveur de connexion View et View Composer à des intervalles réguliers. Dans View Administrator, vous pouvez définir la fréquence et d'autres aspects des opérations de sauvegarde.

Tableau 15-1. Paramètres de sauvegarde de configuration de View Manager

Paramètre	Description
Fréquence de sauvegarde automatique	Toutes les heures. Les sauvegardes sont effectuées toutes les heures. Toutes les 6 heures. Les sauvegardes sont effectuées à minuit, 6 h, midi et 18 h. Toutes les 12 heures. Les sauvegardes sont effectuées à minuit et midi. Tous les jours. Les sauvegardes sont effectuées tous les jours à minuit. Tous les 2 jours. Les sauvegardes sont effectuées à minuit le samedi, le lundi, le mercredi et le vendredi. Toutes les semaines. Les sauvegardes sont effectuées toutes les semaines à minuit le samedi. Toutes les 2 semaines. Les sauvegardes sont effectuées toutes les deux semaines à minuit le samedi. Jamais. Les sauvegardes ne sont pas effectuées automatiquement.
Nombre max. de sauvegardes	Nombre de fichiers de sauvegarde pouvant être stockés sur l'instance de Serveur de connexion View. Le nombre doit être un entier supérieur à 0. Lorsque le nombre maximum est atteint, View Manager supprime le fichier de sauvegarde le plus ancien. Ce paramètre s'applique également aux fichiers de sauvegarde créés lorsque vous utilisez la fonction **[Backup Now (Sauvegarder maintenant)]** .
Emplacement de dossier	Emplacement par défaut des fichiers de sauvegarde sur l'ordinateur où Serveur de connexion View s'exécute : `C:\Programdata\VMWare\VDM\backups` Lorsque vous utilisez la fonction **[Backup Now (Sauvegarder maintenant)]** , View Manager stocke également les fichiers de sauvegarde à cet emplacement.

Exporter des données de configuration depuis Serveur de connexion View

Vous pouvez sauvegarder des données de configuration d'une instance de Serveur de connexion View en exportant le contenu de son référentiel View LDAP.

Vous utilisez la commande `vdmexport` pour exporter les données de configuration View LDAP vers un fichier LDIF crypté. Vous pouvez également utiliser l'option `vdmexport –v` (textuel) pour exporter les données vers un fichier LDIF de texte brut ou l'option `vdmexport –c` (nettoyé) pour exporter les données sous forme de texte brut avec des mots de passe et autres données sensibles supprimés.

Vous pouvez exécuter la commande `vdmexport` sur n'importe quelle instance de Serveur de connexion View. Si vous possédez plusieurs instances de Serveur de connexion View dans un groupe répliqué, vous devez uniquement exporter les données depuis une seule instance. Toutes les instances répliquées contiennent les mêmes données de configuration.

Remarque La commande `vdmexport.exe` sauvegarde uniquement les données View LDAP. Cette commande ne sauvegarde pas les informations sur la base de données View Composer.

Prérequis

- Recherchez le fichier exécutable de la commande `vdmexport.exe` installé avec Serveur de connexion View dans le chemin par défaut.

  ```
  C:\Program Files\VMware\VMware View\Server\tools\bin
  ```

- Ouvrez une session sur une instance de Serveur de connexion View en tant qu'utilisateur dans le rôle Administrateurs ou Administrateurs (lecture seule).

Procédure

1 Sélectionnez **[Démarrer] > [Invite de commande]** .

2 À l'invite de commande, saisissez la commande `vdmexport` et redirigez la sortie vers un fichier. Par exemple :

```
vdmexport > Myexport.LDF
```

Par défaut, les données exportées sont cryptées.

Vous pouvez spécifier le nom du fichier de sortie comme argument de l'option `–f`. Par exemple :

```
vdmexport –f Myexport.LDF
```

Vous pouvez exporter les données au format de texte brut (textuel) à l'aide de l'option `–v`. Par exemple :

```
vdmexport –f Myexport.LDF –v
```

Vous pouvez exporter les données au format de texte brut avec mots de passe et données sensibles supprimés (nettoyé) à l'aide de l'option `–c`. Par exemple :

```
vdmexport –f Myexport.LDF –c
```

Remarque N'envisagez pas d'utiliser des données de sauvegarde nettoyées pour restaurer une configuration View LDAP. Les données de configuration nettoyées ne contiennent pas les mots de passe et autres informations critiques.

Pour plus d'informations sur la commande `vdmexport`, consultez le document *Intégration de VMware Horizon View*.

Suivant

Vous pouvez restaurer ou transférer les informations de configuration de Serveur de connexion View à l'aide de la commande `vdmimport`.

Pour plus d'informations sur l'importation du fichier LDIF, reportez-vous à la section « Restauration des données de configuration de Serveur de connexion View et View Composer », page 407.

Restauration des données de configuration de Serveur de connexion View et View Composer

Vous pouvez restaurer manuellement les fichiers de configuration LDAP de Serveur de connexion View et les fichiers de base de données View Composer qui étaient sauvegardés par View Manager.

Vous exécutez manuellement des utilitaires séparés pour restaurer les données de configuration de Serveur de connexion View et View Composer.

Avant de restaurer des données de configuration, vérifiez que vous avez sauvegardé les données de configuration dans View Administrator. Reportez-vous à la section « Sauvegarde des données de Serveur de connexion View et de View Composer », page 403.

Vous utilisez l'utilitaire `vdmimport` pour importer les données de Serveur de connexion View des fichiers de sauvegarde LDIF vers le référentiel View LDAP dans l'instance de Serveur de connexion View.

Vous pouvez utiliser l'utilitaire `SviConfig` pour importer les données de View Composer des fichiers de sauvegarde `.svi` vers la base de données SQL de View Composer.

Remarque Dans certaines situations, vous pouvez avoir à installer la version actuelle d'une instance de Serveur de connexion View et à restaurer la configuration View existante en important les fichiers de configuration LDAP de Serveur de connexion View. Cette procédure peut être nécessaire dans le cadre d'un plan de continuité d'activité et de reprise d'activité (BC/DR), pour configurer un deuxième datacenter avec la configuration View existante, ou pour d'autres raisons. Pour plus d'informations, consultez la section « Réinstaller Serveur de connexion View avec une configuration de sauvegarde » dans le document *Installation de VMware Horizon View*.

Importer des données de configuration dans Serveur de connexion View

Vous pouvez restaurer des données de configuration d'une instance de Serveur de connexion View en important une copie de sauvegarde des données stockées dans un fichier LDIF.

Vous utilisez la commande `vdmimport` pour importer les données depuis le fichier LDIF vers le référentiel View LDAP dans l'instance de Serveur de connexion View.

Si vous avez sauvegardé votre configuration View LDAP à l'aide de View Administrator ou de la commande `vdmexport` par défaut, le fichier LDIF exporté est crypté. Vous devez décrypter le fichier LDIF pour pouvoir l'importer.

Si le fichier LDIF exporté est au format de texte brut, vous n'avez pas à décrypter le fichier.

Remarque N'importez pas un fichier LDIF au format nettoyé, qui est le texte brut avec mots de passe et autres données sensibles supprimés. Si vous le faites, des informations de configuration critiques manqueront dans le référentiel View LDAP restauré.

Pour plus d'informations sur la sauvegarde du référentiel View LDAP, reportez-vous à la section « Sauvegarde des données de Serveur de connexion View et de View Composer », page 403.

Prérequis

- Recherchez le fichier exécutable de la commande `vdmimport` installé avec Serveur de connexion View dans le chemin par défaut.

  ```
  C:\Program Files\VMware\VMware View\Server\tools\bin
  ```

- Ouvrez une session sur une instance de Serveur de connexion View en tant qu'utilisateur avec le rôle View Administrators.
- Vérifiez que vous connaissez le mot de passe de récupération de données. Si un rappel de mot de passe a été configuré, vous pouvez l'afficher en exécutant la commande `vdmimport` sans l'option de mot de passe.

Procédure

1 Sélectionnez **[Démarrer] > [Invite de commande]** .

2 Décryptez le fichier LDIF crypté.

À l'invite de commande, tapez la commande `vdmimport`. Spécifiez l'option `–d`, l'option `–p` avec le mot de passe de récupération de données et l'option `–f` avec un fichier LDIF crypté existant suivies d'un nom pour le fichier LDIF décrypté. Par exemple :

```
vdmimport –d –p mypassword
–f MyEncryptedexport.LDF > MyDecryptedexport.LDF
```

Si vous ne vous rappelez plus de votre mot de passe de récupération de données, tapez la commande sans l'option `–p`. L'utilitaire affiche le rappel de mot de passe et vous invite à entrer le mot de passe.

3 Importez le fichier LDIF décrypté pour restaurer la configuration View LDAP.

Spécifiez l'option `–f` avec le fichier LDIF décrypté. Par exemple :

```
vdmimport –f MyDecryptedexport.LDF
```

La commande `vdmimport` met à jour le référentiel View LDAP dans Serveur de connexion View avec les données de configuration du fichier LDIF.

Pour plus d'informations sur la commande `vdmimport`, consultez le document *Intégration de VMware Horizon View*.

Restaurer une base de données View Composer

Vous pouvez importer les fichiers de sauvegarde pour votre configuration View Composer dans la base de données View Composer qui stocke les informations du clone lié.

Vous pouvez utiliser la commande `SviConfig restoredata` pour restaurer les données de base de données View Composer après une panne du système ou pour rétablir la configuration de View Composer à un état précédent.

IMPORTANT Seuls les administrateurs expérimentés de View Composer doivent utiliser l'utilitaire `SviConfig`. Cet utilitaire est conçu pour résoudre des problèmes liés au service View Composer.

Prérequis

Vérifiez l'emplacement des fichiers de sauvegarde de base de données View Composer. Par défaut, View Manager stocke les fichiers de sauvegarde sur le lecteur `C:` de l'ordinateur de Serveur de connexion View dans `C:\Programdata\VMWare\VDM\backups`.

Les fichiers de sauvegarde de View Composer utilise une convention de dénomination avec un horodatage et le suffixe `.svi`.

`Backup–`*`YearMonthDayCount–vCenter Server Name_Domain Name`*`.svi`

Par exemple : `Backup–20090304000010–foobar_test_org.svi`

Familiarisez-vous avec les paramètres `SviConfig restoredata` :

- `DsnName` : DSN utilisé pour se connecter à la base de données. Le paramètre DsnName est obligatoire et ne peut pas être une chaîne vide.
- `Username (Nom d'utilisateur)` : nom d'utilisateur utilisé pour se connecter à la base de données. Si vous ne définissez pas ce paramètre, l'authentification Windows est utilisée.
- `Password (Mot de passe)` : mot de passe de l'utilisateur qui se connecte à la base de données. Si vous ne définissez pas ce paramètre et que l'authentification Windows n'est pas utilisée, un message demande ensuite d'entrer le mot de passe.

- `BackupFilePath` : chemin du fichier de sauvegarde View Composer.

Les paramètres `DsnName` et `BackupFilePath` sont obligatoires et ils ne peuvent pas correspondre à une chaîne vide. Les paramètres `Username (Nom d'utilisateur)` et `Password (Mot de passe)` sont facultatifs.

Procédure

1 Copiez les fichiers de sauvegarde de View Composer de l'ordinateur Serveur de connexion View vers un emplacement accessible depuis l'ordinateur où le service View Composer est installé.

2 Sur l'ordinateur où se trouve View Composer, arrêtez le service VMware View Composer.

3 Ouvrez une invite de commande Windows et accédez au fichier exécutable `SviConfig`.

Le fichier est situé avec l'application View Composer.

```
C:\Program Files\VMware\VMware View Composer\sviconfig.exe
```

4 Exécutez la commande `SviConfig restoredata`.

```
sviconfig –operation=restoredata
          –DsnName=target_database_source_name_(DSN)
          –Username=database_administrator_username
          –Password=database_administrator_password
          –BackupFilePath=path_to_View_Composer_backup_file
```

Par exemple :

```
sviconfig –operation=restoredata –dsnname=LinkedClone
–username=Admin –password=Pass
–backupfilepath="C:\Program Files\VMware\VMware View
Composer\Backup–20090304000010–foobar_test_org.SVI"
```

5 Démarrez le service VMware View Composer.

Suivant

Pour voir les codes de résultat de la commande `SviConfig restoredata`, reportez-vous à la section « Codes de résultat pour la restauration de la base de données View Composer », page 409.

Codes de résultat pour la restauration de la base de données View Composer

Lorsque vous restaurez une base de données View Composer, la commande `SviConfig restoredata` affiche un code de résultat.

Tableau 15-2. Codes de résultat de restoredata

Code	Description
0	L'opération a réussi.
1	DSN fourni introuvable.
2	Informations d'identification d'administrateur fournies non valides.
3	Pilote de la base de données non pris en charge.
4	Problème inattendu et échec de la commande.
14	Une autre application utilise le service View Composer. Éteignez le service avant d'exécuter la commande.
15	Un problème s'est produit lors du processus de restauration. Des détails sont disponibles dans la sortie du journal sur l'écran.

Exporter des données dans la base de données View Composer

Vous pouvez exporter des données depuis votre base de données View Composer vers un fichier.

IMPORTANT Utilisez l'utilitaire `SviConfig` uniquement si vous êtes un administrateur View Composer expérimenté.

Prérequis

Par défaut, View Manager stocke les fichiers de sauvegarde sur le lecteur `C:` de l'ordinateur de Serveur de connexion View, à l'emplacement `C:\Programdata\VMWare\VDM\backups`.

Familiarisez-vous avec les paramètres `SviConfig exportdata` :

- `DsnName` : DSN utilisé pour se connecter à la base de données. S'il n'est pas spécifié, le nom DSN, le nom d'utilisateur et le mot de passe seront récupérés depuis le fichier de configuration de serveur.
- `Username` : nom d'utilisateur utilisé pour se connecter à la base de données. Si ce paramètre n'est pas spécifié, l'authentification Windows est utilisée.
- `Password` : mot de passe de l'utilisateur qui se connecte à la base de données. Si ce paramètre n'est pas spécifié et si l'authentification Windows n'est pas utilisée, vous êtes invité à entrer le mot de passe ultérieurement.
- `OutputFilePath` : chemin du fichier de sortie.

Procédure

1 Sur l'ordinateur sur lequel View Composer est installé, arrêtez le service VMware View Composer.

2 Ouvrez une invite de commande Windows et accédez au fichier exécutable SviConfig.

Le fichier est situé avec l'application View Composer.

```
<répertoire d'installation de View Composer>\sviconfig.exe
```

3 Exécutez la commande `SviConfig exportdata`.

```
sviconfig –operation=exportdata
          –DsnName=target_database_source_name_(DSN)
          –Username=database_administrator_username
          –Password=database_administrator_password
          –OutputFilePath=path_to_View_Composer_output_file
```

Par exemple :

```
sviconfig –operation=exportdata –dsnname=LinkedClone
–username=Admin –password=Pass
–outputfilepath="C:\Program Files\VMware\VMware View
Composer\Export–20090304000010–foobar_test_org.SVI"
```

Suivant

Pour exporter les codes de résultat de la commande `SviConfig exportdata`, reportez-vous à la section « Codes de résultat pour l'exportation de la base de données View Composer », page 411.

Codes de résultat pour l'exportation de la base de données View Composer

Lorsque vous exportez une base de données View Composer, la commande `SviConfig exportdata` affiche un code de sortie.

Tableau 15-3. Codes d'Exportdata et d'ExitStatus

Code	Description
0	L'exportation des données s'est terminée avec succès.
1	Le nom DSN fourni est introuvable.
2	Les informations d'identification fournies ne sont pas valides.
3	Pilote non pris en charge pour la base de données fournie.
4	Un problème inattendu s'est produit.
18	Impossible de se connecter au serveur de base de données.
24	Impossible d'ouvrir le fichier de sortie.

Contrôler des composants View

Vous pouvez rapidement contrôler l'état des composants View Manager et vSphere dans votre déploiement View à l'aide du tableau de bord de View Administrator.

View Administrator affiche des informations de contrôle sur des instances de View Connection Server, la base de données des événements, des serveurs de sécurité, des services View Composer, des magasins de données, des instances de vCenter Server et des domaines.

Remarque View Manager ne peut pas déterminer des informations d'état sur les domaines Kerberos. View Administrator affiche l'état du domaine Kerberos comme inconnu, même lorsqu'un domaine est configuré et fonctionne.

Procédure

1 Dans View Administrator, cliquez sur **[Dashboard (Tableau de bord)]** .

2 Dans le volet System Health (Santé du système), développez **[View components (Composants View)]** , **[vSphere components (Composants vSphere)]** ou **[Other components (Autres composants)]** .

- Une flèche vers le haut verte indique qu'un composant n'a pas de problème.
- Une flèche vers le bas rouge indique qu'un composant n'est pas disponible ou qu'il ne fonctionne pas.
- Une double flèche jaune indique qu'un composant est dans un état d'avertissement.
- Un point d'interrogation indique que l'état d'un composant est inconnu.

3 Cliquez sur le nom d'un composant.

Une boîte de dialogue affiche le nom, la version, l'état et d'autres informations sur le composant.

Contrôler l'état du poste de travail

Vous pouvez rapidement contrôler l'état de postes de travail dans votre déploiement View à l'aide du tableau de bord de View Administrator. Par exemple, vous pouvez afficher tous les postes de travail déconnectés ou les postes de travail en mode de maintenance.

Prérequis

Familiarisez-vous avec les états de poste de travail. Reportez-vous à la section « État du poste de travail de machines virtuelles », page 316.

Procédure

1 Dans View Administrator, cliquez sur **[Dashboard (Tableau de bord)]** .

2 Dans le volet Desktop Status (État du poste de travail), développez un dossier d'état.

Option	Description
Preparing (Préparation)	Répertorie les états de poste de travail quand la machine virtuelle est approvisionnée, supprimée ou en mode de maintenance.
Problem Desktops (Postes de travail problématiques)	Répertorie les états d'erreur des postes de travail.
Prepared for use (Préparé pour l'utilisation)	Répertorie les états de poste de travail quand le poste de travail est prêt à être utilisé.

3 Recherchez l'état du poste de travail et cliquez sur le nombre hypertexte se trouvant à côté.

La page **[Desktops (Postes de travail)]** affiche tous les postes de travail avec l'état sélectionné.

Suivant

Vous pouvez cliquer sur un nom de poste de travail pour voir des détails sur ce dernier ou cliquer sur la flèche vers l'arrière de View Administrator pour revenir à la page du tableau de bord.

Comprendre les services View Manager

Le fonctionnement d'instances de Serveur de connexion View et de serveurs de sécurité dépend de plusieurs services qui s'exécutent sur le système. Ces systèmes sont démarrés et arrêtés automatiquement, mais vous pouvez parfois trouver nécessaire d'ajuster le fonctionnement de ces services manuellement.

Vous utilisez l'outil Microsoft Windows Services pour arrêter ou démarrer des services View Manager. Si vous arrêtez des services View Manager sur un hôte de Serveur de connexion View ou un serveur de sécurité, les utilisateurs finaux ne peuvent plus ouvrir de session sur leurs postes de travail jusqu'à ce que vous redémarriez les services. Vous pouvez aussi avoir à redémarrer un service dont l'exécution s'est arrêtée ou si la fonctionnalité de View Manager qu'il contrôle ne répond plus.

Arrêter et démarrer les services View

Le fonctionnement d'instances de Serveur de connexion View et de serveurs de sécurité dépend de plusieurs services qui s'exécutent sur le système. Vous pouvez parfois trouver nécessaire d'arrêter et de démarrer ces services manuellement quand vous utilisez View pour résoudre des problèmes.

Lorsque vous arrêtez des services View, les utilisateurs finaux ne peuvent pas ouvrir de session sur leurs postes de travail. Vous devez effectuer cet arrêt à une heure déjà planifiée pour la maintenance du système, ou avertir les utilisateurs finaux que leurs postes de travail seront temporairement indisponibles.

Remarque Arrêtez uniquement le service VMware Serveur de connexion View sur un hôte de Serveur de connexion View ou le service VMware View Security Server sur un serveur de sécurité. N'arrêtez pas d'autres services de composant.

Prérequis

Familiarisez-vous avec les services exécutés sur des hôtes de Serveur de connexion View et des serveurs de sécurité comme décrit dans les sections « Services sur un hôte de Serveur de connexion View », page 413 et « Services sur un serveur de sécurité », page 414.

Procédure

1 Démarrez l'outil Windows Services en saisissant **`services.msc`** à l'invite de commande.

2 Sélectionnez le service VMware Serveur de connexion View sur un hôte de Serveur de connexion View ou le service VMware View Security Server sur un serveur de sécurité, et cliquez sur **[Arrêter]** , **[Redémarrer]** ou **[Démarrer]** , si nécessaire.

3 Vérifiez que l'état du service répertorié change comme prévu.

Services sur un hôte de Serveur de connexion View

Le fonctionnement de View Manager dépend de plusieurs services s'exécutant sur un hôte de Serveur de connexion View. Si vous voulez ajuster le fonctionnement de ces services, il est important que vous les connaissiez.

Tableau 15-4. Services d'un hôte de Serveur de connexion View

Nom du service	Type de démarrage	Description
Serveur de connexion VMware View	Automatique	Fournit des services de Broker pour les connexions. Ce service doit être exécuté pour le fonctionnement correct de View Manager. Si vous démarrez ou arrêtez ce service, il démarre ou arrête également les services Framework, Message Bus, Security Gateway et Web. Ce service ne démarre ou n'arrête pas les services VMwareVDMDS ou VMware View Script Host.
VMware View Framework Component	Manuel	Fournit des services de journalisation des événements, de sécurité et d'infrastructure COM+ pour View Manager. Ce service doit être exécuté pour le fonctionnement correct de View Manager.
VMware View Message Bus Component	Manuel	Fournit des services de messagerie entre des composants View Manager. Ce service doit être exécuté pour le fonctionnement correct de View Manager.
VMware View PCoIP Secure Gateway	Manuel	Fournit des services PCoIP Secure Gateway. Ce service doit être en cours d'exécution si des clients se connectent à Serveur de connexion View via PCoIP Secure Gateway.
Hôte de script de VMware View	Automatique (si activé)	Fournit la prise en charge de scripts tiers s'exécutant lorsque vous supprimez des machines virtuelles. Par défaut, ce service est désactivé. Vous devez activer ce service si vous voulez exécuter des scripts.
VMware View Security Gateway Component	Manuel	Fournit des services de tunnel sécurisés pour View Manager. Ce service doit être exécuté pour le fonctionnement correct de View Manager.
VMware View Web Component	Manuel	Fournit des services Web pour View Manager. Ce service doit être exécuté pour le fonctionnement correct de View Manager.
VMwareVDMDS	Automatique	Fournit des services de répertoire LDAP Web pour View Manager. Ce service doit être exécuté pour le fonctionnement correct de View Manager. Ce service doit également être exécuté lors des mises à niveau de View pour garantir que des données existantes sont migrées correctement.

Services sur un serveur de sécurité

Le fonctionnement de View Manager dépend de plusieurs services s'exécutant sur un serveur de sécurité. Si vous voulez ajuster le fonctionnement de ces services, il est important que vous les connaissiez.

Tableau 15-5. Services de serveur de sécurité

Nom du service	Type de démarrage	Description
VMware View Security Server	Automatique	Fournit des services de serveur de sécurité. Ce service doit être exécuté pour le fonctionnement correct d'un serveur de sécurité. Si vous démarrez ou arrêtez ce service, il démarre ou arrête également les services Framework et Security Gateway.
VMware View Framework Component	Manuel	Fournit des services de journalisation des événements, de sécurité et d'infrastructure COM+. Ce service doit être exécuté pour le fonctionnement correct d'un serveur de sécurité.
VMware View PCoIP Secure Gateway	Manuel	Fournit des services PCoIP Secure Gateway. Ce service doit être en cours d'exécution si des clients se connectent à un serveur de sécurité via PCoIP Secure Gateway.
VMware View Security Gateway Component	Manuel	Fournit des services de tunnel sécurisés. Ce service doit être exécuté pour le fonctionnement correct d'un serveur de sécurité.

Services sur un hôte de View Transfer Server

Les opérations de transfert pour les postes de travail locaux dépendent des services qui s'exécutent sur un hôte de View Transfer Server. Si vous voulez ajuster le fonctionnement de ces services, il est important que vous les connaissiez.

Tous les services installés avec View Transfer Server doivent être en cours d'exécution pour le fonctionnement correct des postes de travail locaux dans View Manager.

Tableau 15-6. Services d'un hôte de View Transfer Server

Nom du service	Type de démarrage	Description
VMware View Transfer Server	Automatique	Fournit des services qui coordonnent les services liés à View Transfer Server. Si vous démarrez ou arrêtez ce service, il démarre ou arrête également les services View Transfer Server Control Service et Framework.
VMware View Transfer Server Control Service	Manuel	Fournit des capacités de gestion pour View Transfer Server et gère la communication avec View Connection Server.
VMware View Framework Component	Manuel	Fournit des services de journalisation des événements, de sécurité et d'infrastructure COM+ pour View Manager.
Service Apache2.2	Automatique	Fournit des capacités de transfert des données pour des ordinateurs client qui exécutent des postes de travail View en mode local. Le service Apache2.2 est démarré lorsque vous ajoutez View Transfer Server à View Manager.

Ajouter des licences à VMware Horizon View

Si les licences actuelles sur un système expirent ou si vous voulez accéder à des fonctions VMware Horizon View actuellement sans licence, vous pouvez utiliser View Administrator pour ajouter des licences.

Vous pouvez ajouter une licence à VMware Horizon View lorsque View Manager est en cours d'exécution. Vous n'avez pas à redémarrer le système, et l'accès aux postes de travail n'est pas interrompu.

Prérequis

Pour le fonctionnement correct de View Manager et des fonctions complémentaires telles que View Composer et des postes de travail locaux, obtenez une clé de licence valide.

Procédure

1 Dans View Administrator, sélectionnez **[Configuration de View] > [Licence produit et utilisation]** et cliquez sur **[Modifier la licence]** .

2 Saisissez le numéro de série de licence et cliquez sur **[OK]** .

La fenêtre Licence produit montre les informations de licence mises à jour.

Mettre à jour des informations utilisateur générales depuis Active Directory

Vous pouvez mettre à jour View Manager avec les informations utilisateur actuelles stockées dans Active Directory. Cette fonction met à jour le nom, le numéro de téléphone, l'e-mail, le nom d'utilisateur et le domaine Windows par défaut des utilisateurs View. Les domaines externes approuvés sont également mis à jour.

Utilisez cette fonction si vous modifiez la liste de domaines externes approuvés dans Active Directory, en particulier si les relations d'approbation modifiées entre des domaines affectent des autorisations d'utilisateur dans View Manager.

Cette fonction analyse Active Directory à la recherche des dernières informations utilisateur et actualise la configuration de View Manager.

Vous pouvez également utiliser la commande `vdmadmin` pour mettre à jour des informations d'utilisateur et de domaine. Reportez-vous à la section « Mise à jour de sécurités extérieures principales à l'aide de l'option -F », page 471.

Prérequis

Vérifiez que vous pouvez ouvrir une session dans View Administrator en tant qu'administrateur avec le privilège **Manage Global Configuration and Policies (Gérer la configuration et les règles générales)** .

Procédure

1 Dans View Administrator, cliquez sur **[Users and Groups (Utilisateurs et groupes)]** .

2 Choisissez de mettre à jour les informations pour tous les utilisateurs ou pour un utilisateur en particulier.

Option	Action
For all users (Pour tous les utilisateurs)	Cliquez sur **[Update General User Information (Mettre à jour les informations utilisateur générales)]** . La mise à jour de tous les utilisateurs et groupes peut prendre un long moment.
For an individual user (Pour un utilisateur en particulier)	a Cliquez sur le nom d'utilisateur à mettre à jour. b Cliquez sur **[Update General User Information (Mettre à jour les informations utilisateur générales)]** .

Migrer View Composer vers un autre ordinateur

Dans certaines situations, vous devrez peut-être migrer un service View Composer vers un nouvel ordinateur Windows Server. Par exemple, vous pouvez migrer View Composer et vCenter Server vers un nouvel hôte ESXi ou un cluster pour développer votre déploiement de View. De plus, View Composer et vCenter Server n'ont pas à être installés sur le même ordinateur Windows Server.

Vous pouvez migrer View Composer depuis l'ordinateur vCenter Server vers un ordinateur autonome ou depuis un ordinateur autonome vers l'ordinateur vCenter Server.

- Instructions de migration de View Composer page 416

  Les étapes à suivre pour migrer le service View Composer varient selon que vous envisagez ou non de conserver les postes de travail de clone lié.

- Migrer View Composer avec une base de données existante page 417

  Lorsque vous migrez View Composer vers un autre ordinateur, si vous prévoyez de conserver vos postes de travail de clone lié actuels, le nouveau service View Composer doit continuer à utiliser la base de données View Composer existante.

- Migrer View Composer sans poste de travail de clone lié page 418

  Si le service View Composer actuel ne gère aucun poste de travail de clone lié, vous pouvez migrer View Composer vers un nouvel ordinateur sans migrer les clés RSA vers le nouvel ordinateur. Le service View Composer migré peut se connecter à la base de données View Composer d'origine ou vous pouvez préparer une nouvelle base de données pour View Composer.

- Préparer Microsoft .NET Framework pour la migration de clés RSA page 419

  Pour utiliser une base de données View Composer existante, vous devez migrer le conteneur de clés RSA entre les ordinateurs. Vous migrez le conteneur de clés RSA à l'aide de l'outil d'inscription ASP.NET IIS fourni avec Microsoft .NET Framework.

- Migrer le conteneur de clés RSA vers le nouveau service View Composer page 420

  Pour utiliser une base de données View Composer existante, vous devez migrer le conteneur de clés RSA de l'ordinateur source sur lequel le service View Composer existant réside vers l'ordinateur sur lequel vous voulez installer le nouveau service View Composer.

Instructions de migration de View Composer

Les étapes à suivre pour migrer le service View Composer varient selon que vous envisagez ou non de conserver les postes de travail de clone lié.

Pour conserver les postes de travail de clone lié dans le déploiement, le service View Composer que vous installez sur le nouvel ordinateur doit continuer d'utiliser la base de données View Composer existante. La base de données View Composer contient les données nécessaires à la création, au provisionnement, à la gestion et à la suppression des clones liés.

Lorsque vous migrez le service View Composer, vous pouvez également migrer la base de données View Composer vers un nouvel ordinateur.

Que vous migriez ou non la base de données View Composer, la base de données doit être configurée sur un ordinateur disponible dans le même domaine que l'ordinateur sur lequel vous installez le nouveau service View Composer ou sur un domaine de confiance.

View Composer crée des paires de clés RSA pour crypter et décrypter des informations d'authentification stockées dans la base de données View Composer. Pour rendre cette source de données compatible avec le nouveau service View Composer, vous devez migrer le conteneur de clés RSA créé par le service View Composer d'origine. Vous devez importer le conteneur de clés RSA sur l'ordinateur sur lequel vous installez le nouveau service.

Si le service View Composer actuel ne gère pas les postes de travail de clone lié, vous pouvez migrer le service sans utiliser le base de données View Composer existante. Il est inutile de migrer les clés RSA, que vous utilisiez ou non la base de données existante.

Remarque Chaque instance du service View Composer doit posséder sa propre base de données View Composer. Plusieurs services View Composer ne peuvent pas partager une base de données View Composer.

Migrer View Composer avec une base de données existante

Lorsque vous migrez View Composer vers un autre ordinateur, si vous prévoyez de conserver vos postes de travail de clone lié actuels, le nouveau service View Composer doit continuer à utiliser la base de données View Composer existante.

Effectuez les étapes de cette procédure lorsque vous migrez View Composer dans les directions suivantes :

- d'un ordinateur vCenter Server vers un ordinateur autonome ;
- d'un ordinateur autonome vers un ordinateur vCenter Server ;
- d'un ordinateur autonome vers un autre ordinateur autonome ;
- d'un ordinateur vCenter Server vers un autre ordinateur vCenter Server.

Lorsque vous migrez le service View Composer, vous pouvez également migrer la base de données View Composer vers un nouvel emplacement. Par exemple, vous devrez peut-être migrer la base de données View Composer si la base de données actuelle se trouve sur un ordinateur vCenter Server que vous migrez également.

Lorsque vous installez le service View Composer sur le nouvel ordinateur, vous devez configurer le service pour qu'il se connecte à la base de données View Composer.

Prérequis

- Familiarisez-vous avec les exigences de migration de View Composer. Reportez-vous à la section « Instructions de migration de View Composer », page 416.
- Familiarisez-vous avec les étapes de migration du conteneur de clés RSA vers le nouveau service View Composer. Reportez-vous aux sections « Préparer Microsoft .NET Framework pour la migration de clés RSA », page 419 et « Migrer le conteneur de clés RSA vers le nouveau service View Composer », page 420.
- Familiarisez-vous avec l'installation du service View Composer. Consultez la section « Installation de View Composer » dans le document *Installation de VMware Horizon View*.
- Familiarisez-vous avec la configuration d'un certificat SSL pour View Composer. Consultez la section « Configuration de certificats SSL pour des serveurs View Server » dans le document *Installation de VMware Horizon View*.
- Familiarisez-vous avec la configuration de View Composer dans View Administrator. Reportez-vous aux sections « Configurer les paramètres de View Composer », page 18 et « Configurer les domaines de View Composer », page 19.

Procédure

1 Désactivez l'approvisionnement de machine virtuelle dans l'instance de vCenter Server associée au service View Composer.

   a Dans View Administrator, cliquez sur **[Configuration de View] > [Serveurs]** .

   b Sous l'onglet vCenter Server, sélectionnez l'instance de vCenter Server et cliquez sur **[Désactiver l'approvisionnement]** .

2 (Facultatif) Migrez la base de données View Composer vers un nouvel emplacement.

Si vous devez effectuer cette étape, contactez votre administrateur de base de données pour obtenir des instructions sur la migration.

3 Désinstallez le service View Composer de l'ordinateur actuel.

4 (Facultatif) Migrez le conteneur de clés RSA vers le nouvel ordinateur.

5 Installez le service View Composer sur le nouvel ordinateur.

Lors de l'installation, spécifiez le nom DSN de la base de données qui était utilisée par le service View Composer d'origine. Spécifiez également le nom d'utilisateur et le mot de passe d'administrateur de domaine qui étaient fournis pour la source de données ODBC pour cette base de données.

Si vous avez migré la base de données, les informations sur le nom DSN et la source de données doivent pointer vers le nouvel emplacement de la base de données. Que vous ayez migré la base de données ou pas, le nouveau service View Composer doit avoir accès aux informations de base de données d'origine concernant les clones liés.

6 Configurez un certificat de serveur SSL pour View Composer sur le nouvel ordinateur.

Vous pouvez copier le certificat qui a été installé pour View Composer sur l'ordinateur d'origine ou installer un nouveau certificat.

7 Dans View Administrator, configurez les nouveaux paramètres de View Composer.

a Dans View Administrator, cliquez sur **[Configuration de View] > [Serveurs]**, sélectionnez l'instance de vCenter Server associée à ce service View Composer et cliquez sur **[Modifier]** .

b Sous l'onglet View Composer, fournissez les nouveaux paramètres de View Composer.

Si vous installez View Composer avec vCenter Server sur le nouvel ordinateur, sélectionnez **[View Composer est co-installé avec vCenter Server]** .

Si vous installez View Composer sur un ordinateur autonome, sélectionnez **[Serveur View Composer Server autonome]** et fournissez le nom de domaine complet de l'ordinateur View Composer, ainsi que le nom d'utilisateur et le mot de passe de l'utilisateur de View Composer.

c Dans le volet Domaines, cliquez sur **[Vérifier les informations sur le serveur]** et ajoutez ou modifiez les domaines View Composer si nécessaire.

d Cliquez sur **[OK]** .

Migrer View Composer sans poste de travail de clone lié

Si le service View Composer actuel ne gère aucun poste de travail de clone lié, vous pouvez migrer View Composer vers un nouvel ordinateur sans migrer les clés RSA vers le nouvel ordinateur. Le service View Composer migré peut se connecter à la base de données View Composer d'origine ou vous pouvez préparer une nouvelle base de données pour View Composer.

Prérequis

- Familiarisez-vous avec l'installation du service View Composer. Consultez la section « Installation de View Composer » dans le document *Installation de VMware Horizon View*.
- Familiarisez-vous avec la configuration d'un certificat SSL pour View Composer. Consultez la section « Configuration de certificats SSL pour des serveurs View Server » dans le document *Installation de VMware Horizon View*.
- Familiarisez-vous avec les étapes de suppression de View Composer de View Manager. Reportez-vous à la section « Supprimer View Composer de View Manager », page 26.

Avant de pouvoir supprimer View Composer, vérifiez qu'il ne gère plus aucun poste de travail de clone lié. S'il reste des clones liés, vous devez les supprimer.

- Familiarisez-vous avec la configuration de View Composer dans View Administrator. Reportez-vous aux sections « Configurer les paramètres de View Composer », page 18 et « Configurer les domaines de View Composer », page 19.

Procédure

1 Dans View Administrator, supprimez View Composer de View Manager.

   a Dans la boîte de dialogue Modifier un serveur vCenter Server, assurez-vous que **[Ne pas utiliser View Composer]** est sélectionné.

   b Dans la boîte de dialogue Modifier vCenter Server, cliquez sur **[OK]** .

2 Désinstallez le service View Composer de l'ordinateur actuel.

3 Installez le service View Composer sur le nouvel ordinateur.

   Lors de l'installation, configurez View Composer pour qu'il se connecte au nom DSN de la base de données View Composer d'origine ou nouvelle.

4 Configurez un certificat de serveur SSL pour View Composer sur le nouvel ordinateur.

   Vous pouvez copier le certificat qui a été installé pour View Composer sur l'ordinateur d'origine ou installer un nouveau certificat.

5 Dans View Administrator, configurez les nouveaux paramètres de View Composer.

   a Dans View Administrator, cliquez sur **[Configuration de View] > [Serveurs]** , sélectionnez l'instance de vCenter Server associée à ce service View Composer et cliquez sur **[Modifier]** .

   b Dans le volet Paramètres de View Composer Server, cliquez sur **[Modifier]** .

   c Fournissez les nouveaux paramètres de View Composer.

      Si vous installez View Composer avec vCenter Server sur le nouvel ordinateur, sélectionnez **[View Composer est co-installé avec vCenter Server]** .

      Si vous installez View Composer sur un ordinateur autonome, sélectionnez **[Serveur View Composer Server autonome]** et fournissez le nom de domaine complet de l'ordinateur View Composer, ainsi que le nom d'utilisateur et le mot de passe de l'utilisateur de View Composer.

   d Dans le volet Domaines, cliquez sur **[Vérifier les informations sur le serveur]** et ajoutez ou modifiez les domaines View Composer si nécessaire.

   e Cliquez sur **[OK]** .

Préparer Microsoft .NET Framework pour la migration de clés RSA

Pour utiliser une base de données View Composer existante, vous devez migrer le conteneur de clés RSA entre les ordinateurs. Vous migrez le conteneur de clés RSA à l'aide de l'outil d'inscription ASP.NET IIS fourni avec Microsoft .NET Framework.

Prérequis

Téléchargez .NET Framework et apprenez-en plus sur l'outil d'inscription ASP.NET IIS aux emplacements suivants :

- http://www.microsoft.com/net
- http://msdn.microsoft.com/library/k6h9cz8h(VS.80).aspx

Procédure

1 Installez .NET Framework sur l'ordinateur sur lequel le service View Composer associé à la base de données existante est installé.

2 Installez .NET Framework sur l'ordinateur de destination sur lequel vous voulez installer le nouveau service View Composer.

Suivant

Migrez le conteneur de clés RSA vers l'ordinateur de destination. Reportez-vous à la section « Migrer le conteneur de clés RSA vers le nouveau service View Composer », page 420.

Migrer le conteneur de clés RSA vers le nouveau service View Composer

Pour utiliser une base de données View Composer existante, vous devez migrer le conteneur de clés RSA de l'ordinateur source sur lequel le service View Composer existant réside vers l'ordinateur sur lequel vous voulez installer le nouveau service View Composer.

Vous devez effectuer cette procédure avant d'installer le nouveau service View Composer.

Prérequis

Vérifiez que les outils d'enregistrement Microsoft .NET Framework et ASP.NET IIS sont installés sur les ordinateurs source et de destination. Reportez-vous à la section « Préparer Microsoft .NET Framework pour la migration de clés RSA », page 419.

Procédure

1 Sur l'ordinateur source sur lequel réside le service View Composer existant, ouvrez une invite de commande et allez dans le répertoire `%windir%\Microsoft.NET\Framework\v2.0`*`xxxxx`*.

2 Saisissez la commande `aspnet_regiis` pour enregistrer la paire de clés RSA dans un fichier local.

```
aspnet_regiis -px "SviKeyContainer" "keys.xml" -pri
```

L'outil d'inscription ASP.NET IIS exporte la paire de clés publique/privée RSA du conteneur `SviKeyContainer` vers le fichier `keys.xml` et enregistre le fichier en local.

3 Copiez le fichier `keys.xml` vers l'ordinateur de destination sur lequel vous voulez installer le nouveau service View Composer.

4 Sur l'ordinateur de destination, ouvrez une invite de commande et allez dans le répertoire `%windir%\Microsoft.NET\Framework\v2.0`*`xxxxx`*.

5 Saisissez la commande `aspnet_regiis` pour migrer les données de la paire de clés RSA.

```
aspnet_regiis -pi "SviKeyContainer" "path\keys.xml" -exp
```

où *path* est le chemin vers le fichier exporté.

L'option `-exp` crée une paire de clés exportable. Si une future migration est requise, les clés peuvent être exportées depuis cet ordinateur et importées vers un autre ordinateur. Si vous avez précédemment migré les clés vers cet ordinateur sans utiliser l'option `-exp`, vous pouvez de nouveau importer les clés à l'aide de l'option `-exp` afin de pouvoir exporter les clés dans le futur.

L'outil d'inscription importe les données de paire de clés dans le conteneur de clés local.

Suivant

Installez le nouveau service View Composer sur l'ordinateur de destination. Fournissez les informations sur le nom DSN et la source de données ODBC qui permettent à View Composer de se connecter aux mêmes informations de base de données que celles utilisées par le service View Composer d'origine. Pour plus d'informations sur l'installation, consultez la section « Installation de View Composer » dans le document *Installation de VMware Horizon View*.

Effectuez les étapes pour migrer View Composer vers un nouvel ordinateur et utiliser la même base de données. Reportez-vous à la section « Migrer View Composer avec une base de données existante », page 417.

Mettre à jour les certificats sur une instance de Serveur de connexion View, un serveur de sécurité ou View Composer

Lorsque vous recevez des certificats SSL de serveur ou des certificats intermédiaires mis à jour, vous importez les certificats dans le magasin de certificats de l'ordinateur local Windows sur chaque hôte de Serveur de connexion View, du serveur de sécurité ou de View Composer.

En général, les certificats de serveur expirent au bout de 12 mois. Les certificats racine et intermédiaires expirent au bout de 5 ou 10 ans.

Pour plus d'informations sur l'importation des certificats de serveur et intermédiaires, consultez la section « Configurer Serveur de connexion View, le serveur de sécurité ou View Composer pour utiliser un nouveau certificat SSL » dans le document *Installation de VMware Horizon View*.

Prérequis

- Obtenez des certificats de serveur et intermédiaires mis à jour auprès de l'autorité de certification avant l'expiration des certificats actuellement valides.
- Vérifiez que le composant logiciel Certificat a été ajouté à MMC sur l'ordinateur Windows Server sur lequel l'instance de Serveur de connexion View, le serveur de sécurité ou le service View Composer a été installé(e).

Procédure

1 Importez le certificat de serveur SSL signé dans le magasin de certificats de l'ordinateur local Windows sur l'hôte Windows Server.

   a Dans le composant logiciel Certificat, importez le certificat de serveur dans le dossier **[Certificats (ordinateur local)] > [Personnel] > [Certificats]** .

   b Sélectionnez **[Marquer cette clé comme exportable]** .

   c Cliquez sur **[Suivant]** et sur **[Terminer]** .

2 Pour Serveur de connexion View ou le serveur de sécurité, supprimez le nom convivial du certificat, **[vdm]** , de l'ancien certificat qui a été délivré à View Server.

   a Cliquez avec le bouton droit sur l'ancien certificat et cliquez sur **[Propriétés]** .

   b Sous l'onglet Général, supprimez le nom convivial, **[vdm]** .

3 Pour Serveur de connexion View ou le serveur de sécurité, ajoutez le nom convivial du certificat, **[vdm]** , au nouveau certificat qui remplace le précédent.

   a Cliquez avec le bouton droit sur le nouveau certificat et cliquez sur **[Propriétés]** .

   b Sous l'onglet Général, dans le champ Nom convivial, tapez **[vdm]** .

   c Cliquez sur **[Appliquer]** puis sur **[OK]** .

4 Pour un certificat de serveur délivré à View Composer, exécutez l'utilitaire `SviConfig ReplaceCertificate` pour lier le nouveau certificat au port utilisé par View Composer.

   Cet utilitaire remplace la liaison de l'ancien certificat par la liaison du nouveau certificat.

   a Arrêtez le service View Composer.

   b Dans une invite de commande Windows, tapez la commande `SviConfig ReplaceCertificate`. Par exemple :

   ```
   sviconfig –operation=ReplaceCertificate
             –delete=false
   ```

   L'utilitaire affiche une liste numérotée de certificats SSL qui sont disponibles dans le magasin de certificats de l'ordinateur local Windows.

   c Pour sélectionner un certificat, tapez le numéro du certificat et appuyez sur Entrée.

5 Si des certificats intermédiaires sont délivrés à un hôte de Serveur de connexion View, du serveur de sécurité ou de View Composer, importez la mise à jour la plus récente des certificats intermédiaires dans le dossier **[Certificats (ordinateur local)] > [Autorités de certification intermédiaires] > [Certificats]** dans le magasin de certificats Windows.

6 Redémarrez le service Serveur de connexion View, le service du serveur de sécurité ou le service View Composer pour que vos modifications prennent effet.

Informations collectées par le programme d'amélioration de l'expérience du client

Vous pouvez participer à un programme d'amélioration de l'expérience du client lorsque vous installez Serveur de connexion View avec une nouvelle configuration ou en utilisant View Administrator après l'installation. Si vous participez au programme, VMware collecte des données anonymes sur votre déploiement afin d'améliorer la réponse de VMware aux besoins du client. Aucune donnée identifiant votre entreprise n'est collectée.

Avant de collecter des données, VMware rend anonyme tous les champs qui contiennent des informations sur votre entreprise. Les champs expurgés identifient les ordinateurs, le stockage de données, les fonctions réseau, les applications et les utilisateurs. Par exemple, les adresses IP et les spécifications de personnalisation des postes de travail sont rendues anonymes.

VMware expurge un champ en générant un hachage de la valeur réelle. Lorsqu'une valeur de hachage est collectée, VMware ne peut pas identifier la valeur réelle, mais peut détecter ses modifications lorsque vous changez d'environnement.

Pour déterminer si vous voulez participer au programme, vous pouvez vérifier les champs dont les données sont collectées par VMware. Vous pouvez également examiner tous les champs expurgés. Les champs sont organisés par le composant View.

Données View globales collectées par VMware

Si vous participez au programme d'amélioration de l'expérience du client, VMware collecte des données globales sur votre environnement. Les champs contenant des données sensibles sont rendus anonymes.

Tableau 15-7. Données globales collectées pour le programme d'amélioration de l'expérience du client

Description	S'agit-il d'un champ anonyme ?	Exemple de valeur
Les View servers peuvent contacter le contrôleur de domaine.	Non	True ou false
Le DNS du domaine Active Directory	Oui	Aucune

Tableau 15-7. Données globales collectées pour le programme d'amélioration de l'expérience du client (suite)

Description	S'agit-il d'un champ anonyme ?	Exemple de valeur
Le domaine est un domaine de type NT4.	Non	True ou false
Le nom de domaine	Oui	Aucune
L'état du domaine	Non	OK
Le type de relation de confiance avec le domaine	Non	Domaine principal, bidirectionnel, forêt bidirectionnelle, etc.

Données Serveur de connexion View collectées par VMware

Si vous participez au programme d'amélioration de l'expérience du client, VMware collecte les données de certains champs Serveur de connexion View. Les champs contenant des données sensibles sont rendus anonymes.

Tableau 15-8. Données Serveur de connexion View collectées pour le programme d'amélioration de l'expérience du client

Description	S'agit-il d'un champ anonyme ?	Exemple de valeur
Nom commun (CN) de l'entrée Serveur de connexion View dans View LDAP	Oui	Aucune
Serveur de connexion View est désactivé	Non	True ou false
L'authentification SecureID est configurée et active	Non	True ou false
Type d'installation de Serveur de connexion View	Non	0 = Serveur de connexion View 1 = serveur de sécurité
Le nom d'authentification SecureID doit-il correspondre au nom Active Directory ?	Non	True = nom d'authentification SecureID mappé False = nom d'authentification SecureID non mappé
Les clients sont-ils autorisés à ignorer le tunnel sécurisé ?	Non	True ou false
Les clients sont-ils autorisés à ignorer la passerelle sécurisée PCoIP ?	Non	True ou false
Configuration de l'authentification par carte à puce	Non	Désactivé, Facultatif ou Requis
Les utilisateurs doivent-ils être automatiquement déconnectés lorsque leur carte à puce est retirée ?	Non	True ou false
Dossier dans lequel les sauvegardes View LDAP sont stockées	Oui	Aucune
Unité de temps pour définir la fréquence des sauvegardes View LDAP	Non	Heure, Jour ou Semaine
Fréquence des sauvegardes View LDAP	Non	Entier
Heure de sauvegarde View LDAP	Non	Entier
Nombre maximal de sauvegardes LDAP à stocker	Non	Entier
Heure de la dernière sauvegarde View LDAP	Non	Feb 21, 2012 12:00:10 AM
État de la dernière sauvegarde View LDAP	Non	OK
Sauvegarde View LDAP immédiate en attente	Non	True ou false

Tableau 15-8. Données Serveur de connexion View collectées pour le programme d'amélioration de l'expérience du client (suite)

Description	S'agit-il d'un champ anonyme ?	Exemple de valeur
Paramètres de configuration du mode local	Non	Utiliser une connexion tunnel sécurisée pour des opérations en mode local = True ou false Utiliser une connexion tunnel sécurisée modifiable pour les opérations en mode local = True ou False Utiliser SSL pour les opérations en mode local = True ou False Utiliser SSL lors du provisionnement des packages d'images de base pour les postes de travail en mode local = True ou False Utiliser la compression pour les opérations en mode local = True ou False Utiliser la duplication pour les opérations en mode local = True ou False
Balises associées à l'instance de Serveur de connexion View	Oui	Aucune
Si l'instance de Serveur de connexion View est couplée ou non à un serveur de sécurité	Non	0 = Non couplé 1 = Couplé
Nom unique (DN) de l'instance de Serveur de connexion View dans LDAP	Oui	Aucune
Durée de validité du mot de passe du couplage du serveur de sécurité	Non	
Nom d'hôte/de noeud de l'instance de Serveur de connexion View	Oui	Aucune
Numéro de version uniquement de l'instance de Serveur de connexion View	Non	5.1.0
Build et version complètes de l'instance de Serveur de connexion View	Non	5.1.0-123455
Reconnexion automatique à la passerelle sécurisée	Non	True ou false
Protocole TCP (Tunnel Client Protocol)	Non	
Protocole que l'instance de Serveur de connexion View ou le serveur de sécurité écoute	Non	
Numéro de build de l'instance de Serveur de connexion View	Non	123456
Nom du groupe répliqué Serveur de connexion View, généralement le nom de noeud de la première instance de Serveur de connexion View	Oui	Aucune
Nom DNS de l'instance de Serveur de connexion View	Oui	Aucune
Adresse IP de l'instance de Serveur de connexion View	Oui	Aucune
Nom d'hôte NetBIOS de l'instance de Serveur de connexion View	Oui	Aucune
Nombre actuel de postes de travail empruntés	Non	Entier
Nombre maximal de postes de travail empruntés	Non	Entier

Tableau 15-8. Données Serveur de connexion View collectées pour le programme d'amélioration de l'expérience du client (suite)

Description	S'agit-il d'un champ anonyme ?	Exemple de valeur
Nombre actuel de sessions dans l'instance de Serveur de connexion View	Non	Entier
Nombre maximal de sessions dans l'instance de Serveur de connexion View	Non	Entier
Nombre actuel de sessions View Composer dans l'instance de Serveur de connexion View	Non	Entier
Nombre maximal de sessions View Composer dans l'instance de Serveur de connexion View	Non	Entier
Version de l'instance de Serveur de connexion View	Non	5.1.0
Nombre d'appels de cmdlets PowerShell individuelles	Non	Liste d'entiers
Fréquence de connexion en utilisant des mots de passe, dans le temps	Non	Flottant
Fréquence de connexion en utilisant le certificat de serveur SSL, dans le temps	Non	Flottant
Pourcentage d'utilisation moyenne du processeur	Non	Entier
Pourcentage d'utilisation moyenne de la mémoire	Non	Entier

Tableau 15-9. Informations d'état collectées dans Serveur de connexion View pour le programme d'amélioration de l'expérience du client

Description	S'agit-il d'un champ anonyme ?	Exemple de valeur
Numéro de build de l'instance de Serveur de connexion View	Non	123456
Nom du groupe répliqué Serveur de connexion View, généralement le nom de noeud de la première instance de Serveur de connexion View	Oui	Aucune
Nom DNS de l'instance de Serveur de connexion View	Oui	Aucune
Adresse IP de l'instance de Serveur de connexion View	Oui	Aucune
Nom d'hôte NetBIOS de l'instance de Serveur de connexion View	Oui	Aucune
Nombre actuel de postes de travail empruntés	Non	Entier
Nombre maximal de postes de travail empruntés	Non	Entier
Nombre actuel de sessions dans l'instance de Serveur de connexion View	Non	Entier
Nombre maximal de sessions dans l'instance de Serveur de connexion View	Non	Entier
Nombre actuel de sessions View Composer dans l'instance de Serveur de connexion View	Non	Entier
Nombre maximal de sessions View Composer dans l'instance de Serveur de connexion View	Non	Entier
Version de l'instance de Serveur de connexion View	Non	5.1.0

Tableau 15-10. Données d'utilisation dynamiques collectées dans Serveur de connexion View pour le programme d'amélioration de l'expérience du client

Description	S'agit-il d'un champ anonyme ?	Exemple de valeur
Nombre d'appels de cmdlets PowerShell individuelles	Non	Liste d'entiers
Fréquence de connexion en utilisant des mots de passe, dans le temps	Non	Flottant
Fréquence de connexion en utilisant le certificat de serveur SSL, dans le temps	Non	Flottant
Pourcentage d'utilisation moyenne du processeur	Non	Entier
Pourcentage d'utilisation moyenne de la mémoire	Non	Entier

Données de Serveur de sécurité collectées par VMware

Si vous participez au programme d'amélioration de l'expérience du client, VMware collecte les données de certains champs du Serveur de sécurité. Les champs contenant des données sensibles sont rendus anonymes.

Tableau 15-11. Données du Serveur de sécurité collectées pour le programme d'amélioration de l'expérience du client

Description	S'agit-il d'un champ anonyme ?	Exemple de valeur
Le nombre de sessions PCoIP exécutées sur la passerelle sécurisée du Serveur de sécurité	Non	Entier
Le nombre de sessions de n'importe quel type exécutées sur la passerelle sécurisée du Serveur de sécurité	Non	Entier
Le numéro de build du Serveur de sécurité	Non	123456
Le nom d'hôte du Serveur de sécurité	Oui	Aucune
IPsec est actif.	Non	True ou false
La passerelle sécurisée est arrêtée.	Non	True ou false
Le nombre actuel de sessions	Non	Entier
L'URL de la passerelle sécurisée	Oui	Aucune
Le numéro de version du Serveur de sécurité	Non	5.1.0

Données de pool de postes de travail collectées par VMware

Si vous participez au programme d'amélioration de l'expérience du client, VMware collecte des données de certains champs des pools de postes de travail View. Les champs contenant des données sensibles sont rendus anonymes.

Tableau 15-12. Données de pool de postes de travail View collectées pour le programme d'amélioration de l'expérience du client

Description	S'agit-il d'un champ anonyme ?	Exemple de valeur
Nom commun de l'entrée du pool de postes de travail dans View LDAP	Oui	Aucune
Nom d'affichage descriptif du pool de postes de travail	Oui	Aucune
Le pool de postes de travail est désactivé	Non	True ou false

Tableau 15-12. Données de pool de postes de travail View collectées pour le programme d'amélioration de l'expérience du client (suite)

Description	S'agit-il d'un champ anonyme ?	Exemple de valeur
Type du pool de postes de travail	Non	L'un des éléments suivants : `IndividualVC`, `IndividualUnmanaged`, `Persistent`, `NonPersistent`, `SviPersistent`, `SviNonPersistent`, `ManualVCPersistent`, `Manual`, `ManualUnmanagedPersistent`, `ManualUnmanagedNonPersistent`, `TerminalService`, `TransferServer`, `OnRequestVcPersistent`, `OnRequestVcNonPersistent`, `OnRequestSviPersistent`, `OnRequestSviNonPersistent`
Dossier View Administrator dans lequel se trouve le pool de postes de travail	`Oui`	Aucune
Liste des noms uniques de machine virtuelle qui appartiennent au pool de postes de travail	Non	Exemple de liste d'éléments : `["CN=8f11d7cf-b0ef-43ad-92ce-691aa929d3c4,OU=Servers,DC=vdi,DC=vmware,DC=int"]`
Plusieurs sessions sont-elles autorisées dans le pool de postes de travail ?	Non	True ou false
Les utilisateurs du pool de postes de travail sont-ils autorisés à réinitialiser leurs postes de travail ?	Non	Désactivé, Facultatif ou Requis
Délai après lequel un message de fermeture de session forcée s'affiche	Non	True ou false
Nom unique de l'instance vCenter Server qui gère les postes de travail du pool	Non	`"CN=e7a718de-d0f7-444a-9452-156dce289028,OU=VirtualCenter,OU=Properties,DC=vdi,DC=vmware,DC=int"`
Nombre minimal de postes de travail dans le pool	Non	Entier
Nombre maximal de postes de travail dans le pool	Non	Entier
Nombre de postes de travail provisionnés de rechange dans le pool	Non	Entier
Stratégie de suppression du pool de postes de travail	Non	Default, DeleteOnUse ou RefreshOnUse
Suffixe DNS utilisé dans le provisionnement	`Oui`	Aucune
Modèle de dénomination (préfix) à utiliser pour les noms des machines virtuelles autodéployés	`Oui`	Aucune
Modèle utilisé pour cloner les machines virtuelles	`Oui`	Aucune
Dossier dans vCenter Server dans lequel les machines virtuelles déployées sont stockées	`Oui`	Aucune
Pool de ressources utilisé pour les machines virtuelles	`Oui`	Aucune
Liste des magasins de données	`Oui`	Aucune
Spécification de personnalisation utilisée pour déployer les machines virtuelles	`Oui`	Aucune

Tableau 15-12. Données de pool de postes de travail View collectées pour le programme d'amélioration de l'expérience du client (suite)

Description	S'agit-il d'un champ anonyme ?	Exemple de valeur
Activer le provisionnement automatique pour le pool de postes de travail	Non	True ou false
Erreurs lors du provisionnement	Non	
Arrêter le provisionnement en cas d'erreur	Non	True ou false
Démarrer le provisionnement	Non	True ou false
Les valeurs de pool ont été calculées	Non	True ou false
Machine virtuelle parente utilisée pour provisionner les clones liés	Oui	Aucune
Nom de snapshot utilisé pour le provisionnement de clone lié	Oui	Aucune
ID de snapshot utilisé pour le provisionnement de clone lié	Non	`"snapshot-38685"`
ID de groupe de déploiement utilisé par le service View Composer	Non	`"7119316f-00a8-463d-bbba-c3000f105aeb"`
Chemin du magasin de données du disque persistant View Composer	Oui	Aucune
Type de disque View Composer	Non	`"SystemDisposable"`, `UserProfile`, etc.
Créer le disque persistant comme disque de rechange	Non	True ou false
Lettre de montage de lecteur du disque persistant ou du disque de données supprimable	Non	`"*"`, `"C"`, etc.
Taille cible du disque persistant	Non	Entier
Type de stratégie d'actualisation	Non	Toujours, Jamais ou Conditionnel
Seuil d'utilisation des opérations d'actualisation	Non	Entier
Seuil de délai des opérations d'actualisation	Non	Entier
Niveau de surcharge d'un magasin de données qui stocke les clones liés	Non	Aucun, Conservateur, Modéré, Agressif
Chemin d'un magasin de données qui stocke les clones liés	Oui	Aucune
Liste des ID pour laquelle le magasin de données est utilisé	Non	Liste des GUID, telle que : `["7119316f-00a8-463d-bbba-c3000f105aeb"]`
Chaîne de packages Serveur de transfert View publiés hors ligne	Non	
État de poste de travail	Non	Prêt, Pré-provisionné, Clonage, Erreur de clonage Personnalisation, Suppression, Maintenance, Erreur ou Déconnexion
Affecter un poste de travail à un utilisateur lorsque l'utilisateur ouvre une session pour la première fois	Non	True ou false
Marques pour ce pool	Non	
Paramètres de configuration multi-écran	Non	`svga.maxWidth:int`, `svga.vramSize:int`, `svga.maxHeight:int`, `svga.enable3d:bool`, `svga.numDisplays:int`

Tableau 15-12. Données de pool de postes de travail View collectées pour le programme d'amélioration de l'expérience du client (suite)

Description	S'agit-il d'un champ anonyme ?	Exemple de valeur
Un poste de travail individuel a été converti en pool manuel	Non	True ou false
Le pool de clone lié utilise le clonage de snapshot natif avec VAAI	Non	True ou false
CBRC est activé	Non	True ou false
Fréquence d'actualisation du cache CBRC	Non	Entier
Périodes d'indisponibilité de l'actualisation du cache CBRC	Non	Liste
Types de disques mis en cache pour CBRC (disques SE, disques persistants)	Non	Liste

Données de poste de travail collectées par VMware

Si vous participez au programme d'amélioration de l'expérience utilisateur, VMware collecte des données depuis les champs du poste de travail View et depuis les champs de vCenter Server qui décrivent les machines virtuelles de poste de travail. Les champs contenant des informations sensibles restent anonymes.

Tableau 15-13. Données collectées depuis des postes de travail View pour le programme d'amélioration de l'expérience utilisateur

Description	Ce champ reste-t-il anonyme ?	Exemple de valeur
Le poste de travail a été marqué comme endommagé. Le poste de travail a été utilisé lorsque `useonce=true`, il ne doit donc pas accepter de nouvelles sessions	Non	Vrai ou faux
Le poste de travail a été emprunté pour une utilisation en mode local	Non	Vrai ou faux
Le GUID qui identifie la session hors ligne	`Oui`	Aucune
L'utilisateur qui a emprunté le poste de travail	`Oui`	Aucune
État d'un poste de travail utilisé en mode local	Non	Restitué, Emprunté
Le type de transfert de données entre un client et le datacenter	Non	Restitution complète, Répliquer et rester hors ligne
Détermine si une réplication a été demandée par View Administrator	Non	Défini ou Non défini
L'heure à laquelle la réplication explicite a été demandée	Non	Heure
L'heure à laquelle la session hors ligne actuelle du poste de travail a démarré	Non	Heure
Le nom d'hôte de l'ordinateur client qui a emprunté le poste de travail	`Oui`	Aucune
L'adresse IP de l'ordinateur client qui a emprunté le poste de travail	`Oui`	Aucune
L'heure à laquelle le poste de travail hors ligne a reçu une mise à jour des stratégies pour la dernière fois	Non	Heure
ID de snapshot utilisé pour le mode local	`Oui`	Aucune
Liste d'ID de snapshot utilisés pour le mode local	`Oui`	Aucune

Tableau 15-13. Données collectées depuis des postes de travail View pour le programme d'amélioration de l'expérience utilisateur (suite)

Description	Ce champ reste-t-il anonyme ?	Exemple de valeur
Mappage de périphériques pour modifier des ID	Non	Un ensemble d'ID comme le suivant : `2000=01874583;01874583&2016=3910f513;3910f513`
Le poste de travail hors ligne attend une restauration	Non	Vrai ou faux
L'heure à laquelle le poste de travail est passé hors ligne (non mis à jour par des réplications)	Non	Date
Identifiant pour la machine virtuelle utilisée pour corréler les données	Non	vm-10
La personnalisation Sysprep est utilisée pour le poste de travail	Non	Vrai ou faux
Valeur du délai d'expiration. Période de temps avant la déconnexion du poste de travail.	Non	Heure
ID aléatoire pour View Agent pour ce poste de travail	Non	GUID
Diverses valeurs de configuration	Non	Entiers ou booléens (vrai ou faux)
Le GUID du package d'image de base utilisé pour le poste de travail hors ligne	Non	GUID
L'ID du point de terminaison qui a emprunté le poste de travail	`Oui`	Aucune
Identifiant de View LDAP pour le disque persistant de View Composer précédent	Non	Entrée LDAP
Applications ThinApp autorisées sur le poste de travail	`Oui`	Aucune
Applications ThinApp qui attendent une désinstallation	`Oui`	Aucune
Applications ThinApp installées sur le poste de travail	`Oui`	Aucune
L'état du poste de travail	Non	Non défini, Pré-approvisionné, Clonage, Erreur de clonage, Personnalisation, Prêt, Suppression, Maintenance, Erreur ou Fermeture de session
Horodatage du démarrage de la personnalisation	Non	Entier
La machine virtuelle est activée pour la personnalisation	Non	Entier. Les valeurs sont 0 ou 1.
La machine virtuelle est activée	Non	Vrai ou faux
La machine virtuelle est interrompue	Non	Vrai ou faux
L'état de la machine virtuelle est en transition	Non	Vrai ou faux
La machine virtuelle est configurée	Non	Vrai ou faux
Le chemin d'accès à la machine virtuelle dans vCenter Server	`Oui`	Aucune
Modèle de personnalisation utilisé pour personnaliser le poste de travail	`Oui`	Aucune
ID de clone lié de View Composer pour le poste de travail	Non	GUID du clone lié
La machine virtuelle est manquante dans vCenter Server	Non	Vrai ou faux
Nombre de fois que View a tenté de désactiver la machine virtuelle	Non	Entier
État de CBRC	Non	Désactivé, Actuel, Obsolète ou Erreur
Heure de la dernière actualisation CBRC	Non	Date

Tableau 15-13. Données collectées depuis des postes de travail View pour le programme d'amélioration de l'expérience utilisateur (suite)

Description	Ce champ reste-t-il anonyme ?	Exemple de valeur
Heure de la dernière erreur CBRC	Non	Entier
Heure de la dernière tentative incomplète de configuration de CBRC	Non	Entier
La version de View Agent sur le poste de travail	Non	5.1.0-551711
View Persona Management est activé sur le poste de travail	Non	Vrai ou faux

Tableau 15-14. Données de machine virtuelle de poste de travail collectées depuis vCenter Server pour le programme d'amélioration de l'expérience utilisateur

Description	Ce champ reste-t-il anonyme ?	Exemple de valeur
La version matérielle de machine virtuelle	Non	v8
La quantité de RAM allouée à la machine virtuelle	Non	1024
Le nombre de processeurs virtuels configurés dans la machine virtuelle	Non	Entier
Le système d'exploitation installé dans la machine virtuelle	Non	Microsoft Windows 7 (32 bits), Microsoft Windows 8 (32 bits), Microsoft Windows Server 2008 R2 (64 bits), etc.

Données vCenter Server collectées par VMware

Si vous participez au programme d'amélioration de l'expérience du client, VMware collecte les données de certains champs vCenter Server. Les champs contenant des données sensibles sont rendus anonymes.

Tableau 15-15. Données de système hôte et d'état collectées par vCenter Server pour le programme d'amélioration de l'expérience du client

Description	S'agit-il d'un champ anonyme ?	Exemple de valeur
Heure de la dernière communication de View avec l'hôte vCenter Server	Non	Entier
URL de l'instance de vCenter Server.	`Oui`	Aucune
Version d'API de l'instance de vCenter Server.	Non	5.0
Numéro de build de l'instance de vCenter Server.	Non	456789
Numéro de version de l'instance de vCenter Server.	Non	5.0.0
Code d'état interne de l'état de connexion entre vCenter Server et Serveur de connexion View	Non	Status_Up
Description du code d'état de connexion	Non	Connecté
Le certificat SSL vCenter Server est valide.	Non	True ou false
Raison pour laquelle le certificat SSL n'est pas valide	Non	Discordance de nom, non autorisé, ne peut pas vérifier la vérification, etc.

Tableau 15-16. Données de magasin de données collectées depuis vCenter Server pour le programme d'amélioration de l'expérience du client

Description	S'agit-il d'un champ anonyme ?	Exemple de valeur
Capacité de disque du magasin de données	Non	Entier
Espace disque libre dans le magasin de données	Non	Entier
Type de stockage	Non	NFS, VMFS
Plusieurs hôtes peuvent accéder simultanément au magasin de données.	Non	True ou false

Données Serveur de transfert View et du référentiel de Serveur de transfert collectées par VMware

Si vous participez au programme d'amélioration de l'expérience du client, VMware collecte les données des champs Serveur de transfert View et des champs qui décrivent le référentiel Transfert Server. Les champs contenant des données sensibles sont rendus anonymes.

Tableau 15-17. Données Serveur de transfert View et du référentiel de Serveur de transfert collectées par le programme d'amélioration de l'expérience du client

Description	S'agit-il d'un champ anonyme ?	Exemple de valeur
Nom d'hôte de l'instance de Serveur de transfert View	Oui	Aucune
Nombre de transfert actifs	Non	Entier
Chemin d'accès au référentiel de Serveur de transfert Il s'agit d'un champ Serveur de transfert View.	Oui	Aucune
État de l'instance de Serveur de transfert View	Non	Prêt, Maintenance ou Erreur
Quantité totale d'espace disque sur l'ordinateur virtuel Serveur de transfert View	Non	Entier
Quantité totale d'espace disque utilisée sur l'ordinateur virtuel Serveur de transfert View	Non	Entier
Version et numéro de build de l'instance de Serveur de transfert View	Non	5.0.0.123456
Chemin d'accès au référentiel de Serveur de transfert Il s'agit d'un champ LDAP View global.	Oui	Aucune
Quantité d'espace disque utilisée dans le référentiel de Serveur de transfert	Non	Entier
Quantité d'espace disque libre dans le référentiel de Serveur de transfert	Non	Entier
Point de montage sur l'instance de Serveur de transfert View Server	Oui	Aucune

Résolution des problèmes des composants View 16

Vous pouvez utiliser plusieurs procédures pour le diagnostic et la résolution de problèmes que vous pouvez rencontrer lorsque vous utilisez View Manager, View Composer et View Client.

Les administrateurs peuvent rencontrer un comportement inattendu lorsqu'ils utilisent View Manager et View Composer, et les utilisateurs peuvent faire face à des difficultés lorsqu'ils utilisent View Client pour accéder à leurs postes de travail. Vous pouvez utiliser des procédures de dépannage pour rechercher les causes de tels problèmes et essayer de les corriger vous-même, ou vous pouvez obtenir de l'aide du support technique de VMware.

Ce chapitre aborde les rubriques suivantes :

Contrôle de la santé du système

Vous pouvez utiliser le tableau de bord de santé du système dans View Administrator pour voir rapidement les problèmes pouvant affecter le fonctionnement de View ou l'accès à des postes de travail par des utilisateurs finaux.

Le tableau de bord de santé du système en haut à gauche de l'écran de View Administrator fournit un nombre de liens que vous pouvez utiliser pour voir des rapports sur le fonctionnement de View Manager :

Remote Sessions (Sessions distantes)	Fournit un lien vers l'écran Global Remote Sessions (Sessions distantes générales) qui affiche des informations sur l'état des sessions distantes.
Local Sessions (Sessions locales)	Fournit un lien vers l'écran Global Local Sessions View (Sessions View locales générales) qui affiche des informations sur l'état de sessions de poste de travail locales.
Problem Desktops (Postes de travail problématiques)	Fournit un lien vers l'écran Global Desktop View (Poste de travail View général) qui affiche des informations sur les postes de travail indiqués par View Manager comme ayant des problèmes.
Events (Événements)	Fournit des liens vers l'écran Events (Événements) filtré pour des événements d'erreur et pour des événements d'avertissement.
System Health (Santé du système)	Fournit des liens vers l'écran Dashboard (Tableau de bord) qui affiche des résumés sur l'état des composants View, des composants vSphere, des domaines, des postes de travail et sur l'utilisation des magasins de données.

Le tableau de santé du système affiche un lien numéroté à côté de chaque élément. Cette valeur indique le nombre d'éléments sur lesquels le rapport lié fournit des détails.

Contrôler des événements dans View Manager

La base de données des événements stocke des informations sur les événements qui surviennent dans l'hôte ou le groupe Serveur de connexion View, View Agent et View Administrator, et vous informe du nombre d'événements dans le tableau de bord. Vous pouvez examiner les événements en détail sur l'écran Événements.

Remarque Les événements sont listés dans l'interface View Administrator pour une période limitée. Après cette durée, les événements ne sont disponibles que dans les tableaux de base de données historiques. Vous pouvez utiliser des outils de rapport de base de données de Microsoft SQL Server ou d'Oracle pour examiner des événements dans les tableaux de base de données. Pour plus d'informations, consultez le document *Intégration de VMware Horizon View*.

En plus de contrôler des événements dans View Administrator, vous pouvez générer des événements View au format `Syslog` pour qu'un logiciel d'analyse puisse accéder aux données d'événement. Consultez les sections « Génération de messages de journal des événements View au format Syslog à l'aide de l'option -I », page 474 et « Configurer la journalisation des événements pour des serveurs Syslog » dans le document *Installation de VMware Horizon View*.

Prérequis

Créez et configurez la base de données des événements comme décrit dans le document *Installation de VMware Horizon View*.

Procédure

1 Dans View Administrator, sélectionnez **[Contrôle] > [Événements]** .

2 (Facultatif) Dans la fenêtre Événements, vous pouvez sélectionner la période des événements, appliquer des filtres aux événements et trier les événements répertoriés sur une ou plusieurs colonnes.

Messages d'événement de View Manager

View Manager signale des événements dès que l'état du système change ou qu'il rencontre un problème. Vous pouvez utiliser les informations dans les messages d'événement pour effectuer l'action appropriée.

Tableau 16-1 montre les types d'événements signalés par View Manager.

Tableau 16-1. Types d'événements signalés par View Manager

Type d'événement	Description
Échec de l'audit ou Succès de l'audit	Signale l'échec ou le succès d'une modification qu'un administrateur ou un utilisateur fait au fonctionnement ou à la configuration de View.
Erreur	Signale une opération échouée par View Manager.
Informations	Signale des opérations normales dans View.
Avertissement	Signale des problèmes mineurs avec des opérations ou des paramètres de configuration qui peuvent mener à des problèmes plus sérieux dans le temps.

Vous devrez peut-être effectuer certaines actions si vous voyez des messages associés à des événements Échec de l'audit, Erreur ou Avertissement. Vous n'avez pas à effectuer d'actions pour les événements Succès de l'audit ou Information.

Envoyer des messages à des utilisateurs de poste de travail

Vous devez parfois avoir à envoyer des messages à des utilisateurs dont la session est actuellement ouverte sur des postes de travail. Par exemple, si vous devez effectuer de la maintenance sur des postes de travail, vous pouvez demander aux utilisateurs de fermer leur session temporairement ou les prévenir d'une future interruption de service. Vous pouvez envoyer un message à plusieurs utilisateurs.

Procédure

1 Dans View Administrator, cliquez sur **[Inventaire] > [Pools]** .

2 Double-cliquez sur un pool et cliquez sur l'onglet **[Sessions]** .

3 Sélectionnez un ou plusieurs postes de travail et cliquez sur **[Envoyer un message]** .

4 Saisissez le message, sélectionnez le type de message et cliquez sur **[OK]** .

Un message peut être du type **[Infos]** , **[Avertissement]** ou **[Erreur]** .

Le message est envoyé à tous les postes de travail sélectionnés dans des sessions actives.

Afficher les postes de travail avec des problèmes suspects

Vous pouvez afficher une liste des postes de travail pour lesquels View Manager a détecté un fonctionnement suspect.

View Administrator affiche des postes de travail présentant les problèmes suivants :

- Allumés mais ne répondent pas.
- Restent dans l'état d'approvisionnement pendant un long moment.
- Sont prêts mais signalent qu'ils n'acceptent pas les connexions.

- Apparaissent manquants sur un serveur vCenter Server.
- Ont des connexions actives sur la console, des connexions par des utilisateurs non autorisés ou des connexions non effectuées via une instance de Serveur de connexion View.

Procédure

1 Dans View Administrator, sélectionnez **[Postes de travail]** .

2 Sous l'onglet **[VM VirtualCenter]** , cliquez sur **[Postes de travail problématiques]** .

Suivant

L'action que vous devez prendre dépend du problème signalé par View Administrator pour un poste de travail.

- Si le plug-in View Desktops a été ajouté à vSphere Web Client, vous pouvez utiliser vSphere Web Client pour rechercher un utilisateur View, afficher les postes de travail associés à cet utilisateur et dépanner les machines virtuelles sous-jacentes dans vCenter Server. Reportez-vous à la section « Dépanner une machine virtuelle de poste de travail problématique à l'aide de vSphere Web Client », page 436.
- Si un poste de travail de clone lié est dans un état d'erreur, le mécanisme de récupération automatique de View Manager tente d'activer, ou d'arrêter et de redémarrer, le clone lié. Si des tentatives de récupération répétées échouent, le clone lié est supprimé. Dans certaines situations, un clone lié peut être supprimé et recréé plusieurs fois. Reportez-vous à la section « Dépannage de postes de travail qui sont supprimés et recréés plusieurs fois », page 454.
- Si un poste de travail est mis sous tension, mais qu'il ne répond pas, redémarrez sa machine virtuelle. Si le poste de travail ne répond toujours pas, vérifiez que la version de View Agent est prise en charge pour le système d'exploitation du poste de travail. Reportez-vous à la section « Configuration de la journalisation dans View Agent à l'aide de l'option -A », page 468.
- Si un poste de travail reste dans l'état d'approvisionnement pendant un long moment, supprimez sa machine virtuelle et clonez-la de nouveau. Vérifiez que l'espace disque est suffisant pour approvisionner le poste de travail. Reportez-vous à la section « Des machines virtuelles sont bloquées dans l'état d'approvisionnement », page 450.
- Si un poste de travail signale qu'il est prêt, mais qu'il n'accepte pas les connexions, vérifiez la configuration du pare-feu pour vous assurer que le protocole d'affichage (RDP ou PCoIP) n'est pas bloqué. Reportez-vous à la section « Problèmes de connexion entre des postes de travail et des instances de View Connection Server », page 445.
- Si un poste de travail apparaît manquant sur un serveur vCenter Server, vérifiez si sa machine virtuelle est configurée sur le serveur vCenter Server attendu ou si elle a été déplacée vers un autre serveur vCenter Server.
- Si un poste de travail a une connexion active, mais qu'elle n'est pas sur la console, la session doit être distante. Si vous ne pouvez pas contacter les utilisateurs connectés, vous devrez peut-être redémarrer la machine virtuelle pour fermer les sessions des utilisateurs de force.

Dépanner une machine virtuelle de poste de travail problématique à l'aide de vSphere Web Client

Si un poste de travail View présente un problème, vous pouvez utiliser la fonction View Desktops dans vSphere Web Client pour rechercher un utilisateur de View, afficher le poste de travail de l'utilisateur et résoudre des problèmes avec la machine virtuelle sous-jacente dans vCenter Server.

Par exemple, si un utilisateur appelle avec un problème tel qu'un poste de travail qui s'exécute lentement, vous pouvez immédiatement accéder à la machine virtuelle de l'utilisateur sur la page Machines virtuelles dans vSphere Web Client et résoudre le problème.

Prérequis

- Vérifiez que le plug-in View Desktops a été ajouté à vSphere Web Client. Consultez la section « Ajout du plug-in View Desktops à vSphere Web Client » dans le document *Installation de VMware Horizon View*.
- Vérifiez que vous pouvez ouvrir une session sur vSphere Web Client en tant qu'utilisateur avec le rôle Administrateurs View ou Administrateurs View (lecture seule) et avec le privilège Administrateur vSphere pour les machines virtuelles de poste de travail View et les dossiers vCenter Server qui stockent les machines virtuelles.

  Si vous recherchez des postes de travail sans disposer du privilège Administrateur vSphere, les noms de machine virtuelle sont affichés sous forme de liens désactivés et vous ne pouvez pas accéder aux informations de machine virtuelle.

Procédure

1 Ouvrez une session sur vSphere Web Client en tant qu'utilisateur avec le rôle Administrateurs View ou Administrateurs View (lecture seule) et les privilèges Administrateur vSphere appropriés.

  Par exemple : **`https://vSphere_Web_Client_IP_address_or_FQDN:9443/vsphere-client/`**

2 Dans la zone Rechercher, tapez le nom d'un utilisateur de View.

3 Sélectionnez le nom d'utilisateur dans les résultats de la recherche.

4 Sélectionnez un poste de travail associé à l'utilisateur dans la liste de postes de travail.

5 Allez à la page Machines virtuelles pour voir des détails sur la machine virtuelle de poste de travail sous-jacente.

Gérer des postes de travail et des règles pour des utilisateurs non autorisés

Vous pouvez afficher les postes de travail alloués à des utilisateurs dont l'autorisation a été supprimée. Vous pouvez également afficher les règles qui ont été appliquées à des utilisateurs non autorisés.

Un utilisateur non autorisé peut avoir quitté l'entreprise définitivement ou vous pouvez avoir suspendu son compte pour une longue période de temps. Ces utilisateurs sont affectés à un poste de travail mais ils ne sont plus autorisés à utiliser le pool de postes de travail.

Vous pouvez également utiliser la commande `vdmadmin` pour afficher des postes de travail non autorisés et des règles. Reportez-vous à la section « Affichage des postes de travail et des règles d'utilisateurs non autorisés à l'aide des options -O et -P », page 485.

Procédure

1 Dans View Administrator, sélectionnez **[Desktops (Postes de travail)]** .

2 Sélectionnez **[Plus de commandes]** > **[Afficher les postes de travail non autorisés]** .

3 Supprimez les affectations de poste de travail d'utilisateurs non autorisés et restaurez des postes de travail locaux que des utilisateurs non autorisés ont empruntés.

4 Sélectionnez **[Plus de commandes]** > **[Afficher les postes de travail non autorisés]** ou **[Plus de commandes]** > **[Afficher les règles non autorisées]** si nécessaire.

5 Modifiez ou supprimez les règles qui sont appliquées à des utilisateurs non autorisés.

Collecte d'informations de diagnostic pour VMware Horizon View

Vous pouvez collecter des informations de diagnostic pour aider le support technique de VMware à diagnostiquer et résoudre les problèmes avec VMware Horizon View.

Vous pouvez collecter des informations de diagnostic pour plusieurs composants de View. La façon de collecter ces informations varie en fonction du composant View.

- Créer un groupe DCT pour View Agent page 438

  Pour aider le support technique de VMware à résoudre les problèmes de View Agent, vous devrez peut-être utiliser la commande `vdmadmin` pour créer un groupe DCT (Data Collection Tool). Vous pouvez également obtenir le groupe DCT manuellement, sans utiliser `vdmadmin`.

- Enregistrer des informations de diagnostic pour View Client page 439

  Si vous rencontrez des problèmes lors de l'utilisation de View Client, et que vous ne pouvez pas résoudre ces problèmes avec des techniques de dépannage de réseau générales, vous pouvez enregistrer une copie des fichiers journaux et des informations sur la configuration.

- Collecter des informations de diagnostic pour View Composer à l'aide du script de support page 440

  Vous pouvez utiliser le script de support View Composer pour collecter des données de configuration et générer des fichiers journaux pour View Composer. Ces informations aident le support client de VMware à diagnostiquer des problèmes se produisant avec View Composer.

- Collecter des informations de diagnostic pour View Connection Server à l'aide de l'outil de support page 440

  Vous pouvez utiliser l'outil de support pour définir des niveaux de journalisation et générer des fichiers journaux pour View Connection Server.

- Collecter des informations de diagnostic pour View Agent, View Client ou Serveur de connexion View dans la console page 441

  Si vous avez un accès direct à la console, vous pouvez utiliser les scripts de support pour générer des fichiers journaux pour Serveur de connexion View, View Client ou des postes de travail exécutant View Agent. Ces informations aident le support technique de VMware à diagnostiquer des problèmes se produisant avec ces composants.

Créer un groupe DCT pour View Agent

Pour aider le support technique de VMware à résoudre les problèmes de View Agent, vous devrez peut-être utiliser la commande `vdmadmin` pour créer un groupe DCT (Data Collection Tool). Vous pouvez également obtenir le groupe DCT manuellement, sans utiliser `vdmadmin`.

Pour votre convenance, vous pouvez utiliser la commande `vdmadmin` sur une instance de Serveur de connexion View pour demander un groupe DCT à partir d'un poste de travail View. Le groupe est renvoyé à Serveur de connexion View.

Vous pouvez également vous connecter à un poste de travail View spécifique et exécuter une commande `support` qui crée le groupe DCT sur ce poste de travail. Si le système d'exploitation du poste de travail View est Windows 8 ou Windows 7 et que le Contrôle de compte d'utilisateur est activé, vous devez obtenir le groupe DCT de cette façon.

Procédure

1 Connectez-vous en tant qu'utilisateur avec les privilèges requis.

Option	Action
Sur Serveur de connexion View, à l'aide de vdmadmin	Ouvrez une session sur une instance standard ou réplica de Serveur de connexion View en tant qu'utilisateur avec le rôle **Administrateurs** .
Sur le poste de travail View	Ouvrez une session sur le poste de travail View en tant qu'utilisateur avec des privilèges d'administration.

2 Ouvrez une invite de commande et exécutez la commande pour générer le groupe DCT.

Option	Action
Sur Serveur de connexion View, à l'aide de vdmadmin	Pour spécifier les noms du fichier de groupe de sortie, du pool de postes de travail et de la machine, utilisez les options `–outfile`, `–d` et `–m` avec la commande `vdmadmin`. `vdmadmin –A [–b` *`authentication_arguments`*`] –getDCT –outfile` *`local_file`* `–d` *`desktop`* `–m` *`machine`*
Sur le poste de travail View	Modifiez les répertoires vers `c:\Program Files\VMware\VMware View\Agent\DCT` et exécutez la commande suivante : `support`

La commande inscrit le groupe sur le fichier de sortie spécifié.

Exemple : Exemple d'utilisation de vdmadmin pour créer un fichier de groupe pour View Agent

Créez le groupe DCT pour la machine machine1 dans le pool de postes de travail dtpool2 et inscrivez-le dans le fichier zip `C:\myfile.zip`.

```
vdmadmin –A –d dtpool2 –m machine1 –getDCT –outfile C:\myfile.zip
```

Suivant

Si vous avez une demande de support existante, vous pouvez la mettre à jour en joignant le fichier de groupe DCT.

Enregistrer des informations de diagnostic pour View Client

Si vous rencontrez des problèmes lors de l'utilisation de View Client, et que vous ne pouvez pas résoudre ces problèmes avec des techniques de dépannage de réseau générales, vous pouvez enregistrer une copie des fichiers journaux et des informations sur la configuration.

Vous pouvez essayer de résoudre les problèmes de connexion pour View Client avant d'enregistrer les informations de diagnostic et de contacter le support technique de VMware. Pour plus d'informations, reportez-vous à la section « Problèmes de connexion entre View Client et View Connection Server », page 443.

Procédure

1 Dans View Client, cliquez sur **[Informations de support]** , ou dans le menu du poste de travail virtuel, sélectionnez **[Options]** > **[Informations de support]** .

2 Dans la fenêtre Informations de support, cliquez sur **[Collecter des données de support]** puis sur **[Oui]** .

Une fenêtre de commande affiche la progression de la collecte d'informations. Ce processus peut prendre plusieurs minutes.

3 Dans la fenêtre de commande, suivez les invites en saisissant les URL des instances de Serveur de connexion View avec lesquelles vous voulez tester la configuration de View Client et, si nécessaire, en choisissant de générer un diagnostic des processus de View.

   Les informations sont inscrites dans un fichier zip enregistré dans un dossier, sur le poste de travail de la machine client.

4 Classez une demande de support sur la page Support du site Web de VMware et joignez le fichier zip de sortie.

Collecter des informations de diagnostic pour View Composer à l'aide du script de support

Vous pouvez utiliser le script de support View Composer pour collecter des données de configuration et générer des fichiers journaux pour View Composer. Ces informations aident le support client de VMware à diagnostiquer des problèmes se produisant avec View Composer.

Prérequis

Ouvrez une session sur l'ordinateur sur lequel View Composer est installé.

Comme vous devez utiliser l'utilitaire Windows Script Host (`cscript`) pour exécuter le script de support, familiarisez-vous avec l'utilisation de `cscript`. Reportez-vous à la section http://technet.microsoft.com/library/bb490887.aspx.

Procédure

1 Ouvrez une fenêtre d'invite de commande et sélectionnez le répertoire `C:\Program Files\VMware\VMware View Composer`.

   Si vous n'avez pas installé le logiciel dans les répertoires par défaut, utilisez la lettre de disque et le chemin appropriés.

2 Saisissez la commande pour exécuter le script `svi-support`.

```
cscript ".\svi-support.wsf" /zip
```

   Vous pouvez utiliser l'option `/?` pour afficher des informations sur d'autres options de commande qui sont disponibles avec le script.

   Lorsque le script se termine, il vous informe du nom et de l'emplacement du fichier de sortie.

3 Classez une demande de support sur la page Support du site Web de VMware et joignez le fichier de sortie.

Collecter des informations de diagnostic pour View Connection Server à l'aide de l'outil de support

Vous pouvez utiliser l'outil de support pour définir des niveaux de journalisation et générer des fichiers journaux pour View Connection Server.

L'outil de support collecte des données de journalisation pour View Connection Server. Ces informations aident le support technique de VMware à diagnostiquer des problèmes se produisant avec View Connection Server. L'outil de support n'est pas conçu pour collecter des informations de diagnostic pour View Client ou View Agent. À la place, vous devez utiliser le script de support. Reportez-vous à la section « Collecter des informations de diagnostic pour View Agent, View Client ou Serveur de connexion View dans la console », page 441.

Prérequis

Ouvrez une session sur une instance standard ou réplica de View Connection Server en tant qu'utilisateur dans le rôle **Administrators (Administrateurs)** .

Procédure

1 Sélectionnez **[Start (Démarrer)] > [All Programs (Tous les programmes)] > [VMware] > [Set View Connection Server Log Levels (Définir les niveaux de journaux View Connection Server)]** .

2 Dans la zone de texte **[Choice (Choix)]** , saisissez une valeur numérique pour définir le niveau de journalisation et appuyez sur Entrée.

Option	Description
0	Réinitialise le niveau de journalisation sur la valeur par défaut.
1	Sélectionne un niveau normal de journalisation (par défaut).
2	Sélectionne un niveau de débogage de journalisation.
3	Sélectionne la journalisation complète.

Vous devez normalement saisir **2** pour sélectionner un niveau de débogage de journalisation.

Le système démarre l'enregistrement des informations de journal avec le niveau de détail que vous avez sélectionné.

3 Lorsque vous avez collecté suffisamment d'informations sur le comportement de View Connection Server, sélectionnez **[Start (Démarrer)] > [All Programs (Tous les programmes)] > [VMware] > [Generate View Connection Server Log Bundle (Générer un bundle de journaux View Connection Server)]** .

L'outil de support inscrit les fichiers journaux dans un dossier appelé `vdm-sdct` sur le poste de travail de l'instance de View Connection Server.

4 Classez une demande de support sur la page Support du site Web de VMware et joignez les fichiers de sortie.

Collecter des informations de diagnostic pour View Agent, View Client ou Serveur de connexion View dans la console

Si vous avez un accès direct à la console, vous pouvez utiliser les scripts de support pour générer des fichiers journaux pour Serveur de connexion View, View Client ou des postes de travail exécutant View Agent. Ces informations aident le support technique de VMware à diagnostiquer des problèmes se produisant avec ces composants.

Prérequis

Ouvrez une session sur le système pour lequel vous voulez collecter des informations.

- Pour View Agent, ouvrez une session sur la machine virtuelle sur laquelle View Agent est installé.
- Pour View Client, ouvrez une session sur le système sur lequel View Client est installé.
- Pour Serveur de connexion View, ouvrez une session sur l'hôte de Serveur de connexion View.

Procédure

1 Ouvrez une fenêtre d'invite de commande et allez au répertoire approprié pour le composant View pour lequel vous voulez collecter des informations de diagnostic.

Option	Description
View Agent	Passez au répertoire `C:\Program Files\VMware View\Agent\DCT`.
View Client	Passez au répertoire `C:\Program Files\VMware View\Client\DCT`.
Serveur de connexion View	Passez au répertoire `C:\Program Files\VMware View\Server\DCT`.

Si vous n'avez pas installé le logiciel dans les répertoires par défaut, utilisez la lettre de disque et le chemin appropriés.

2 Saisissez la commande pour exécuter le script de support.

```
.\support.bat [loglevels]
```

Si vous voulez activer la journalisation avancée, spécifiez l'option `loglevels` et saisissez la valeur numérique pour le niveau de journalisation lorsque vous y êtes invité.

Option	Description
0	Réinitialise le niveau de journalisation sur la valeur par défaut.
1	Sélectionne un niveau normal de journalisation (par défaut).
2	Sélectionne un niveau de débogage de journalisation.
3	Sélectionne la journalisation complète.
4	Sélectionne la journalisation informationnelle pour PCoIP (View Agent et View Client uniquement).
5	Sélectionne la journalisation de débogage pour PCoIP (View Agent et View Client uniquement).
6	Sélectionne la journalisation informationnelle pour des canaux virtuels (View Agent et View Client uniquement).
7	Sélectionne la journalisation de débogage pour des canaux virtuels (View Agent et View Client uniquement).
8	Sélectionne la journalisation de trace pour des canaux virtuels (View Agent et View Client uniquement).

Le script inscrit les fichiers journaux zippés dans le dossier `vdm-sdct` sur le poste de travail.

3 Vous pouvez trouver les journaux d'agent client de View Composer dans le répertoire `C:\Program Files\Common Files\VMware\View Composer Guest Agent svi-ga-support`.

4 Classez une demande de support sur la page Support du site Web de VMware et joignez le fichier de sortie.

Mettre à jour des demandes de support

Vous pouvez mettre à jour votre demande de support existante sur le site Web Support.

Après le classement d'une demande de support, vous pouvez recevoir une demande d'e-mail provenant du support technique de VMware qui vous demande le fichier de sortie des scripts `support` ou `svi-support`. Lorsque vous exécutez les scripts, ils vous informent du nom et de l'emplacement du fichier de sortie. Répondez au message en joignant le fichier de sortie.

Si le fichier de sortie est trop volumineux pour être inclus en pièce jointe (10 Mo ou plus), contactez le support technique de VMware, fournissez le numéro de votre demande de support et demandez des instructions pour télécharger le fichier sur notre site FTP. Vous pouvez également joindre le fichier à votre demande de support existante sur le site Web Support.

Procédure

1 Rendez-vous sur la page Support du site Web VMware et ouvrez une session.

2 Cliquez sur **[Support Request History (Historique des demandes de support)]** et recherchez le numéro de demande de support applicable.

3 Mettez à jour la demande de support et joignez le fichier de sortie obtenu en exécutant le script `support` ou `svi-support`.

Résolution des problèmes de connexion réseau

Vous pouvez utiliser plusieurs procédures pour le diagnostic et la résolution de problèmes liés à des connexions réseau avec des postes de travail, des clients View Client et des instances de View Connection Server.

Problèmes de connexion entre View Client et View Connection Server

Vous pouvez rencontrer des problèmes de connexion entre View Client et View Connection Server.

Problème

Si la connectivité entre View Client et une instance de View Connection Server échoue, vous voyez l'une des erreurs View Client suivantes :

- `A secure connection to the server '`*`servername`*`' cannot be established.` (Une connexion sécurisée au serveur '*servername*' ne peut pas être établie.)
- `The View Connection Server connection failed. (La connexion à View Connection Server a échoué.)`

L'ouverture d'un poste de travail peut également échouer après avoir contacté une instance de View Connection Server et obtenu une liste de postes de travail disponibles.

Cause

Des problèmes de connectivité entre View Client et une instance de View Connection Server peuvent se produire pour différentes raisons.

- Des paramètres de proxy réseau ou de pare-feu incorrects sur View Client.
- Une erreur de recherche du nom DNS de l'hôte de View Connection Server lors de la configuration d'une connexion sécurisée.

Solution

Essayez les solutions suivantes en séquence. Si une solution ne résout pas le problème, essayez la suivante.

- Utilisez un navigateur pour accéder à l'instance de View Connection Server à l'aide de HTTP ou HTTPS.

  Si vous ne voyez pas la page d'ouverture de session, appliquez des techniques de dépannage de réseau générales pour résoudre le problème.
- Saisissez des informations d'identification valides sur la page d'ouverture de session.
- Si vous recevez un message d'erreur sur l'incapacité de démarrer la connexion sécurisée, la raison la plus probable est que View Client (ou un serveur proxy, si configuré) ne peut pas résoudre le nom DNS de l'hôte de View Connection Server. Configurez l'hôte pour qu'il fournisse son adresse IP plutôt que son FQDN lorsqu'il demande à View Client d'ouvrir une connexion sécurisée.

  a Dans View Administrator, cliquez sur **[View Configuration (Configuration de View) > Servers (Serveurs)]** .

  b Sélectionnez l'instance du serveur de sécurité ou de View Connection Server et cliquez sur **[Edit (Modifier)]** .

  c Dans la zone de texte External URL (URL externe), modifiez l'URL pour qu'elle contienne l'adresse IP externe pour l'instance du serveur de sécurité ou de View Connection Server à laquelle les clients View peuvent accéder sur Internet.

  d Cliquez sur **[OK]** .

  L'URL externe est mise à jour immédiatement. Vous n'avez pas à redémarrer le service View Connection Server pour que la modification prenne effet.
- Si la solution précédente ne résout pas le problème, redémarrez l'instance de View Connection Server.

Problèmes de connexion entre View Client et PCoIP Secure Gateway

Vous pouvez rencontrer des problèmes de connexion entre View Client et un hôte du serveur de sécurité ou de Serveur de connexion View lorsque PCoIP Secure Gateway est configuré pour authentifier des utilisateurs externes qui communiquent sur PCoIP.

Problème

Les clients View utilisant PCoIP ne peuvent pas se connecter ou afficher des postes de travail View. La connexion initiale à une instance du serveur de sécurité ou de Serveur de connexion View réussit, mais la connexion échoue lorsque l'utilisateur sélectionne un poste de travail View. Ce problème se produit lorsque PCoIP Secure Gateway est configuré sur un hôte du serveur de sécurité ou de Serveur de connexion View.

Remarque En général, PCoIP Secure Gateway est exploité sur un serveur de sécurité. Dans une configuration de réseau dans laquelle des clients externes se connectent directement à un hôte de Serveur de connexion View, PCoIP Secure Gateway peut également être configuré sur Serveur de connexion View.

Cause

Des problèmes de connexion à PCoIP Secure Gateway peuvent se produire pour différentes raisons.

- Le pare-feu Windows a fermé un port requis pour PCoIP Secure Gateway.
- PCoIP Secure Gateway n'est pas activé sur l'instance du serveur de sécurité ou de Serveur de connexion View.
- Le paramètre PCoIP External URL (URL externe PCoIP) est mal configuré. Vous devez spécifier ce paramètre en tant qu'adresse IP externe à laquelle les clients View peuvent accéder sur Internet.
- L'URL externe PCoIP ou l'URL externe du tunnel sécurisé est configurée pour pointer vers un hôte du serveur de sécurité ou de Serveur de connexion View différent. Lorsque vous configurez ces deux URL externes sur un hôte du serveur de sécurité ou de Serveur de connexion View, les deux URL externes doivent être des adresses de l'hôte actuel.
- Le client View se connecte via un proxy Web externe qui a fermé un port requis pour PCoIP Secure Gateway. Par exemple, un proxy Web sur le réseau d'un hôtel ou une connexion publique sans fil peut bloquer les ports requis.
- La version de l'instance de Serveur de connexion View couplée avec le serveur de sécurité sur lequel PCoIP Secure Gateway est configuré est View 4.5 ou antérieure. La version du serveur de sécurité et de l'instance de Serveur de connexion View couplée doit être View 4.6 ou supérieure.

Solution

- Vérifiez que les ports réseau suivants sont ouverts sur le pare-feu pour l'hôte du serveur de sécurité ou de Serveur de connexion View.

Port	Description
TCP 4172	De View Client vers l'hôte du serveur de sécurité ou de Serveur de connexion View.
UDP 4172	Entre View Client et l'hôte du serveur de sécurité ou de Serveur de connexion View, dans les deux sens.
TCP 4172	De l'hôte du serveur de sécurité ou de Serveur de connexion View vers le poste de travail View.
UDP 4172	Entre l'hôte du serveur de sécurité ou de Serveur de connexion View et le poste de travail View, dans les deux sens.

- Dans View Administrator, activez PCoIP Secure Gateway et assurez-vous que l'URL externe PCoIP est correctement configurée.
  a Cliquez sur **[View Configuration (Configuration de View)] > [Servers (Serveurs)]** .
  b Sélectionnez l'instance du serveur de sécurité ou de Serveur de connexion View et cliquez sur **[Edit (Modifier)]** .
  c Cochez la case **[Use PCoIP Secure Gateway for PCoIP connections to desktop (Utiliser des connexions PCoIP Secure Gateway pour PCoIP vers le poste de travail)]** .

    PCoIP Secure Gateway est désactivé par défaut.
  d Dans la zone de texte **[PCoIP External URL (URL externe PCoIP)]** , assurez-vous que l'URL contient l'adresse IP externe pour l'instance du serveur de sécurité ou de Serveur de connexion View à laquelle les clients View peuvent accéder sur Internet.

    Spécifiez le port 4172. N'incluez pas de nom de protocole.

    Par exemple : **`10.20.30.40:4172`**
  e Assurez-vous que **[PCoIP External URL (URL externe PCoIP)]** et **[External URL (URL externe)]** du tunnel sécurisé sont les adresses que les systèmes client utilisent pour atteindre cet hôte.

    Par exemple, si vous configurez un hôte de Serveur de connexion View, ne spécifiez pas **[PCoIP External URL (URL externe PCoIP)]** pour cet hôte et **[External URL (URL externe)]** du tunnel sécurisé pour un serveur de sécurité couplé.
  f Cliquez sur **[OK]** .
- Si l'utilisateur se connecte via un proxy Web se trouvant à l'extérieur de votre réseau, et que le proxy bloque un port requis, demandez à l'utilisateur de se connecter à partir d'un emplacement réseau différent.
- Assurez-vous que la version du serveur de sécurité et de l'instance de Serveur de connexion View couplée est View 4.6 ou supérieure.

Problèmes de connexion entre des postes de travail et des instances de View Connection Server

Vous pouvez rencontrer des problèmes de connexion entre des postes de travail et des instances de View Connection Server.

Problème

Si la connectivité entre un poste de travail et une instance de View Connection Server échoue, vous voyez l'un des messages suivants dans la base de données des événements.

- `Provisioning error occurred for Machine` *`Machine_Name`*`: Customization error due to no network communication between the View agent and Connection Server (Une erreur d'approvisionnement s'est produite pour la machine` *`Machine_Name`* `: erreur de personnalisation due à une absence de communication réseau entre l'agent View et Connection Server)`
- `Provisioning error occurred on Pool` *`Desktop_ID`* `because of a networking problem with a View Agent (Une erreur d'approvisionnement s'est produite sur le pool` *`Desktop_ID`* `à cause d'un problème de réseau avec un View Agent)`
- `Unable to launch from Pool` *`Desktop_ID`* `for user` *`User_Display_Name`*`: Failed to connect to Machine` *`MachineName`* `using` *`Protocol`* `(Lancement impossible depuis le pool` *`Desktop_ID`* `pour l'utilisateur` *`User_Display_Name`* `: impossible de se connecter à la machine` *`MachineName`* `à l'aide de` *`Protocol`*`)`

Cause

Les problèmes de connectivité entre un poste de travail et une instance de View Connection Server peuvent se produire pour différentes raisons.

- Une erreur de recherche sur le poste de travail pour le nom DNS de l'hôte de View Connection Server.
- Les ports pour la communication JMS, RDP ou AJP13 bloqués par des règles de pare-feu.
- L'échec du routeur JMS sur l'hôte de View Connection Server.

Solution

- À l'invite de commande sur le poste de travail, saisissez la commande `nslookup`.

  `nslookup` *`CS_FQDN`*

  CS_FQDN est le nom de domaine complet (FQDN) de l'hôte de View Connection Server. Si la commande ne parvient pas à renvoyer l'adresse IP de l'hôte de View Connection Server, appliquez des techniques de dépannage de réseau générales pour corriger la configuration DNS.
- À l'invite de commande sur le poste de travail, vérifiez que le port TCP 4001, que View Agent utilise pour établir une communication JMS avec l'hôte de View Connection Server, fonctionne en saisissant la commande `telnet`.

  `telnet` *`CS_FQDN`* `4001`

  Si la connexion `telnet` est établie, la connectivité réseau pour JMS fonctionne.
- Si un serveur de sécurité est déployé dans la zone démilitarisée, vérifiez que les règles d'exception sont configurées dans le pare-feu intérieur pour autoriser la connectivité RDP entre le serveur de sécurité et des machines virtuelles de poste de travail sur le port TCP 3389.
- Si des connexions sécurisées sont dérivées, vérifiez que les règles de pare-feu autorisent un client à établir une connexion RDP directe avec la machine virtuelle de poste de travail sur le port TCP 3389, ou une connexion PCoIP directe avec la machine virtuelle de poste de travail sur le port TCP 4172 et le port UDP 4172.
- Vérifiez que les règles d'exception sont configurées dans le pare-feu intérieur pour autoriser des connexions entre chaque serveur de sécurité et son hôte de View Connection Server associé sur le port TCP 4001 (JMS) et le port TCP 8009 (AJP13).

Problèmes de connexion dus à une affectation incorrecte d'adresses IP à des postes de travail clonés

Vous pouvez ne pas être capable de vous connecter à des postes de travail clonés s'ils ont des adresses IP statiques.

Problème

Vous ne pouvez pas utiliser View Client pour vous connecter à des postes de travail clonés.

Cause

Des postes de travail clonés sont mal configurés pour utiliser une adresse IP statique au lieu d'utiliser DHCP pour obtenir leurs adresses IP.

Solution

1 Vérifiez que le modèle pour un pool de postes de travail sur vCenter est configuré de sorte à utiliser DHCP pour affecter des adresses IP à des postes de travail.

2 Dans VMware Infrastructure Client, clonez une machine virtuelle manuellement depuis le pool de postes de travail et vérifiez qu'elle obtient correctement son adresse IP depuis DHCP.

Résolution des problèmes de création de pool de postes de travail

Vous pouvez utiliser plusieurs procédures pour le diagnostic et la résolution de problèmes liés à la création de pools de postes de travail.

La création de pool échoue si des spécifications de personnalisation sont introuvables

Si vous essayez de créer un pool de postes de travail, l'opération échoue si les spécifications de personnalisation sont introuvables.

Problème

Vous ne pouvez pas créer de pool de postes de travail et vous voyez le message suivant dans la base de données des événements.

`Provisioning error occurred for Machine` *`Machine_Name`*`: Customization failed for Machine (Une erreur d'approvisionnement s'est produite pour la machine` *`Machine_Name`* `: échec de la personnalisation pour la machine)`

Cause

La cause la plus probable de ce problème est que vous disposez d'autorisations insuffisantes pour accéder aux spécifications de personnalisation ou pour créer un pool. Une autre cause possible est que la spécification de personnalisation a été renommée ou supprimée.

Solution

- Vérifiez que vous disposez d'autorisations suffisantes pour accéder aux spécifications de personnalisation et pour créer un pool.
- Si la spécification de personnalisation n'existe plus car elle a été renommée ou supprimée, choisissez une spécification différente.

La création de pool échoue à cause d'un problème d'autorisations

Vous ne pouvez pas créer de pool de postes de travail s'il y a un problème d'autorisations avec un hôte ESX/ESXi, un cluster ESX/ESXi ou le datacenter.

Problème

Vous ne pouvez pas créer de pool de postes de travail dans View Administrator car les modèles, l'hôte ESX/ESXi, le cluster ESX/ESXi ou le datacenter ne sont pas accessibles.

Cause

Ce problème a plusieurs causes possibles.

- Vous ne disposez pas des autorisations correctes pour créer un pool.
- Vous ne disposez pas des autorisations correctes pour accéder aux modèles.
- Vous ne disposez pas des autorisations correctes pour accéder à l'hôte ESX/ESXi, au cluster ESX/ESXi ou au datacenter.

Solution

- Si l'écran Template Selection (Sélection de modèle) n'indique aucun modèle disponible, vérifiez que vous disposez d'autorisations suffisantes pour accéder aux modèles.
- Vérifiez que vous disposez d'autorisations suffisantes pour accéder à l'hôte ESX/ESXi, au cluster ESX/ESXi ou au datacenter.

- Vérifiez que vous disposez d'autorisations suffisantes pour créer un pool.

L'approvisionnement de pool échoue à cause d'un problème de configuration

Si un modèle n'est pas disponible ou qu'une image de machine virtuelle a été déplacée ou supprimée, l'approvisionnement d'un pool de postes de travail peut échouer.

Problème

Un pool de postes de travail n'est pas approvisionné et vous voyez le message suivant dans la base de données des événements.

`Provisioning error occurred on Pool` *`Desktop_ID`* `because of a configuration problem (Une erreur d'approvisionnement s'est produite sur le pool` *`Desktop_ID`* `à cause d'un problème de configuration)`

Cause

Ce problème a plusieurs causes possibles.

- Un modèle n'est pas accessible.
- Le nom d'un modèle a été modifié dans vCenter.
- Un modèle a été déplacé vers un dossier différent dans vCenter.
- Une image de machine virtuelle a été déplacée entre des hôtes ESX/ESXi ou elle a été supprimée.

Solution

- Vérifiez que le modèle est accessible.
- Vérifiez que le nom et le dossier corrects sont spécifiés pour le modèle.
- Si une image de machine virtuelle a été déplacée entre des hôtes ESX/ESXi, déplacez la machine virtuelle vers le bon dossier vCenter.
- Si une image de machine virtuelle a été supprimée, supprimez l'entrée pour la machine virtuelle dans View Administrator et recréez ou restaurez l'image.

L'approvisionnement de pool échoue à cause d'une instance de View Connection Server incapable de se connecter à vCenter

Si un serveur Connection Server ne peut pas se connecter à vCenter, l'approvisionnement d'un pool de postes de travail peut échouer.

Problème

L'approvisionnement d'un pool de postes de travail échoue et vous voyez l'un des messages d'erreur suivants dans la base de données des événements.

- `Cannot log in to vCenter at address` *`VC_Address`* `(Impossible d'ouvrir une session sur vCenter à l'adresse` *`VC_Address`*`)`
- `The status of vCenter at address` *`VC_Address`* `is unknown (L'état de vCenter à l'adresse` *`VC_Address`* `est inconnu)`

Cause

L'instance de View Connection Server ne peut pas se connecter à vCenter pour l'une des raisons suivantes.

- Le service Web sur le serveur vCenter Server s'est arrêté.
- Il existe des problèmes de réseau entre l'hôte de View Connection Server et le serveur vCenter Server.

- Les numéros de port et les informations d'ouverture de session pour vCenter ou View Composer ont été modifiés.

Solution

- Vérifiez que le service Web s'exécute sur le serveur vCenter.
- Vérifiez qu'il n'y a pas de problème de réseau entre l'hôte de View Connection Server et le serveur vCenter.
- Dans View Administrator, vérifiez les numéros de port et les informations d'ouverture de session qui sont configurés pour vCenter et View Composer.

L'approvisionnement de pool échoue à cause de problèmes liés au magasin de données

Si un magasin de données n'a plus d'espace disque ou que vous n'avez pas l'autorisation d'accéder au magasin de données, l'approvisionnement d'un pool de postes de travail peut échouer.

Problème

L'approvisionnement d'un pool de postes de travail échoue et vous voyez l'un des messages d'erreur suivants dans la base de données des événements.

- `Provisioning error occurred for Machine` *`Machine_Name`*`: Cloning failed for Machine (Une erreur d'approvisionnement s'est produite pour la machine` *`Machine_Name`* `: échec du clonage pour la machine)`
- `Provisioning error occurred on Pool` *`Desktop_ID`* `because available free disk space is reserved for linked clones (Une erreur d'approvisionnement s'est produite sur le pool` *`Desktop_ID`* `car l'espace disque libre est réservé aux clones liés)`
- `Provisioning error occurred on Pool` *`Desktop_ID`* `because of a resource problem (Une erreur d'approvisionnement s'est produite sur le pool` *`Desktop_ID`* `à cause d'un problème de ressource)`

Cause

Vous n'avez pas l'autorisation d'accéder au magasin de données sélectionné ou le magasin de données utilisé pour le pool n'a plus d'espace disque.

Solution

- Vérifiez que vous disposez d'autorisations suffisantes pour accéder au magasin de données sélectionné.
- Vérifiez si le disque sur lequel le magasin de données est configuré est plein.
- Si le disque est plein ou si l'espace est réservé, libérez de l'espace sur le disque, rééquilibrez les magasins de données disponibles ou migrez le magasin de données vers un disque plus volumineux.

L'approvisionnement de pool échoue car vCenter Server est surchargé

Si vCenter Server est surchargé par des demandes, l'approvisionnement d'un pool de postes de travail peut échouer.

Problème

L'approvisionnement d'un pool de postes de travail échoue et vous voyez le message d'erreur suivant dans la base de données des événements.

`Une erreur d'approvisionnement s'est produite sur le pool` *`Desktop_ID`* `à cause d'une expiration au cours de la personnalisation`

Cause

vCenter est surchargé par des demandes.

Solution

- Dans View Administrator, réduisez le nombre maximal d'opérations d'approvisionnement et d'alimentation simultanées pour vCenter Server.
- Configurez des instances de vCenter Server supplémentaires.

  Pour plus d'informations sur la configuration de vCenter Server, consultez le document *Installation de VMware Horizon View*.

Des machines virtuelles sont bloquées dans l'état d'approvisionnement

Après leur clonage, des machines virtuelles sont bloquées dans l'état Provisioning (Approvisionnement).

Problème

Des machines virtuelles sont bloquées dans l'état Provisioning (Approvisionnement).

Cause

La cause la plus probable de ce problème est que vous avez redémarré l'instance de View Connection Server au cours d'une opération de clonage.

Solution

- Supprimez les machines virtuelles et clonez-les de nouveau.

Des machines virtuelles sont bloquées dans l'état de personnalisation

Après leur clonage, des machines virtuelles sont bloquées dans l'état Customizing (Personnalisation).

Problème

Des machines virtuelles sont bloquées dans l'état Customizing (Personnalisation).

Cause

La cause la plus probable de ce problème est qu'il n'y a pas suffisamment d'espace disque pour démarrer la machine virtuelle. Une machine virtuelle doit démarrer avant que la personnalisation puisse avoir lieu.

Solution

- Supprimez la machine virtuelle pour restaurer d'une personnalisation bloquée.
- Si le disque est plein, libérez de l'espace sur le disque ou migrez le magasin de données vers un disque plus volumineux.

Résolution d'un couplage échoué d'un serveur de sécurité avec Serveur de connexion View

Un serveur de sécurité peut ne pas fonctionner s'il n'a pas pu être couplé correctement avec une instance de Serveur de connexion View.

Problème

Les problèmes de serveur de sécurité suivants peuvent se produire si un serveur de sécurité n'a pas pu être couplé avec Serveur de connexion View :

- Lorsque vous essayez d'installer le serveur de sécurité une deuxième fois, le serveur de sécurité ne peut pas se connecter à Serveur de connexion View.

- Des View Client ne peuvent pas se connecter à View. Le message d'erreur suivant apparaît : `The View Connection Server authentication failed. No gateway is available to provide a secure connection to a desktop. L'authentification du Serveur de connexion View a échoué. Aucune passerelle n'est disponible pour fournir une connexion sécurisée à un poste de travail. Contactez votre administrateur réseau.`
- Le serveur de sécurité est affiché dans le tableau de bord View Administrator comme étant `nactif`.

Cause

Ce problème peut se produire si vous avez commencé à installer un serveur de sécurité et que la tentative a été annulée ou bien interrompue après que vous avez entré un mot de passe de couplage de serveur de sécurité.

Solution

Si vous prévoyez de garder le serveur de sécurité dans votre environnement View, procédez comme suit :

1 Dans View Administrator, cliquez sur **[Configuration de View] > [Serveurs]** .

2 Sous l'onglet Serveurs de sécurité, sélectionnez un serveur de sécurité et cliquez sur **[Plus de commandes] > [Préparer la mise à niveau ou la réinstallation]** et cliquez sur **[OK]** .

3 Sélectionnez l'onglet Serveurs de connexion, sélectionnez l'instance de Serveur de connexion View que vous voulez coupler avec le serveur de sécurité, cliquez sur **[Plus de commandes] > [Spécifier un mot de passe de couplage de serveur de sécurité]** , entrez un mot de passe et cliquez sur **[OK]** .

4 Installez de nouveau le serveur de sécurité.

Si vous prévoyez de supprimer l'entrée du serveur de sécurité de votre environnement View, exécutez la commande `vdmadmin –S`.

Par exemple : **`vdmadmin –S –r –s security_server_name`**

Résolution de la vérification de la révocation des certificats de View Server

Un serveur de sécurité ou une instance de Serveur de connexion View utilisé(e) pour des connexions View Client sécurisées peut apparaître en rouge dans View Administrator si la vérification de la révocation des certificats ne peut pas être exécutée sur le certificat SSL du serveur.

Problème

L'icône d'un serveur de sécurité ou de Serveur de connexion View est rouge dans le tableau de bord de View Administrator. L'état de View Server affiche le message suivant : `Le certificat du serveur ne peut pas être vérifié`.

Cause

La vérification de la révocation des certificats peut échouer si votre entreprise utilise un serveur proxy pour l'accès Internet, ou si une instance de Serveur de connexion View ne peut pas accéder aux serveurs qui fournissent la vérification de la révocation des certificats à cause de pare-feu ou d'autres contrôles.

Une instance de Serveur de connexion View effectue la vérification de la révocation des certificats sur son propre certificat et sur ceux des serveurs de sécurité couplés avec elle. Par défaut, le service de Serveur de connexion VMware View est démarré avec le compte `LocalSystem`. Lorsqu'elle est exécutée sous `LocalSystem`, une instance de Serveur de connexion View ne peut pas utiliser les paramètres proxy configurés dans Internet Explorer pour accéder à l'URL des points de distribution de listes de révocation des certificats ou au répondeur OCSP afin de déterminer l'état de révocation du certificat.

Vous pouvez utiliser les commandes `Netshell` de Microsoft pour importer les paramètres proxy dans l'instance de Serveur de connexion View afin que le serveur puisse accéder aux sites de vérification de la révocation des certificats sur Internet.

Solution

1 Sur l'ordinateur Serveur de connexion View, ouvrez une fenêtre de ligne de commande avec le paramètre **[Exécuter en tant qu'administrateur]** .

Par exemple, cliquez sur **[Démarrer]** , tapez **cmd**, cliquez avec le bouton droit sur l'icône `cmd.exe` et sélectionnez **[Exécuter en tant qu'administrateur]** .

2 Saisissez **netsh** et appuyez sur Entrée.

3 Saisissez **winhttp** et appuyez sur Entrée.

4 Saisissez **show proxy** et appuyez sur Entrée.

`Netshell` indique que le proxy a été défini sur la connexion directe. Avec ce paramètre, l'ordinateur Serveur de connexion View ne peut pas se connecter à Internet si un proxy est utilisé dans votre entreprise.

5 Configurez les paramètres proxy.

Par exemple, à l'invite `netsh winhttp>`, tapez **import proxy source=ie**.

Les paramètres proxy sont importés dans l'ordinateur Serveur de connexion View.

6 Vérifiez les paramètres proxy en tapant **show proxy**.

7 Redémarrez le service Serveur de connexion VMware View.

8 Sur le tableau de bord de View Administrator, vérifiez que l'icône du serveur de sécurité ou de Serveur de connexion View est verte.

Dépannage de la vérification de la révocation des certificats de carte à puce

L'instance de Serveur de connexion View ou le serveur de sécurité avec la carte à puce connectée ne peut pas effectuer la vérification de la révocation des certificats sur le certificat SSL du serveur sauf si vous avez configuré la vérification de la révocation des certificats de carte à puce.

Problème

La vérification de la révocation des certificats peut échouer si votre entreprise utilise un serveur proxy pour l'accès Internet, ou si une instance de Serveur de connexion View ou un serveur de sécurité ne peut pas accéder aux serveurs qui fournissent la vérification de la révocation des certificats à cause de pare-feu ou d'autres contrôles.

IMPORTANT Vérifiez que le fichier CRL est à jour.

Cause

View prend en charge la vérification de la révocation des certificats avec des listes de révocation de certificats (CRL) et avec le protocole OCSP (Online Certificate Status Protocol). Une CRL est une liste de certificats révoqués publiée par l'autorité de certification qui a émis les certificats. OCSP est un protocole de validation de certificat utilisé pour obtenir l'état de révocation d'un certificat X.509. L'autorité de certification doit être accessible depuis l'hôte de Serveur de connexion View ou l'hôte du serveur de sécurité. Ce problème se produit uniquement si vous avez configuré la vérification de la révocation des certificats de carte à puce. Reportez-vous à la section « Utilisation de la vérification de la révocation des certificats de carte à puce », page 190.

Solution

1 Créez votre propre procédure (manuelle) pour télécharger une CRL à jour depuis le site Web de l'autorité de certification que vous utilisez vers un chemin sur votre View Server.

2 Créez ou modifiez le fichier `locked.properties` dans le dossier de configuration de la passerelle SSL sur l'hôte de Serveur de connexion View ou du serveur de sécurité.

   Par exemple : *`install_directory`*`\VMware\VMware View\Server\sslgateway\conf\locked.properties`

3 Ajoutez les propriétés `enableRevocationChecking` et `crlLocation` dans le fichier `locked.properties` au chemin local dans lequel la CRL est stockée.

4 Redémarrez le service Serveur de connexion View ou le service du Serveur de sécurité pour que vos modifications prennent effet.

Dépannage de problèmes de redirection USB

Plusieurs problèmes peuvent se produire avec la redirection USB dans View Client.

Problème

La redirection USB dans View Client ne peut pas rendre les périphériques locaux disponibles sur le poste de travail distant, ou certains périphériques ne semblent pas être disponibles pour la redirection dans View Client.

Cause

Voici des causes possibles d'échec du fonctionnement correct ou prévu de la redirection USB.

- La redirection USB n'est pas prise en charge pour les systèmes Windows 2003 ou Windows 2008 ou pour les postes de travail View gérés par Microsoft Terminal Services.
- Les webcams ne sont pas prises en charge pour la redirection.
- La redirection de périphériques audio USB dépend de l'état du réseau et n'est pas fiable. Certains périphériques requièrent un débit de données élevé même lorsqu'ils sont inactifs.
- La redirection USB n'est pas prise en charge pour les périphériques d'amorçage. Si vous exécutez View Client sur un système Windows qui s'amorce à partir d'un périphérique USB, et que vous redirigez ce périphérique vers le poste de travail distant, le système d'exploitation local peut ne plus répondre ou devenir inutilisable. Reportez-vous à la section http://kb.vmware.com/kb/1021409.
- Par défaut, View Client pour Windows ne permet pas de sélectionner un clavier, une souris, une carte à puce et un périphérique de sortie audio pour les rediriger. Reportez-vous à la section http://kb.vmware.com/kb/1011600.
- RDP ne prend pas en charge la redirection pour les périphériques HID USB pour la session de console, ou pour les lecteurs de cartes à puce. Reportez-vous à la section http://kb.vmware.com/kb/1011600.
- Windows Mobile Device Center peut empêcher la redirection de périphériques USB pour des sessions RDP. Reportez-vous à la section http://kb.vmware.com/kb/1019205.
- Pour certains périphériques HID USB, vous devez configurer la machine virtuelle afin d'actualiser la position du pointeur de la souris. Reportez-vous à la section http://kb.vmware.com/kb/1022076.
- Pour certains périphériques audio, vous devrez éventuellement modifier les paramètres de règle ou de Registre. Reportez-vous à la section http://kb.vmware.com/kb/1023868.
- La latence réseau peut ralentir l'interaction entre périphériques ou rendre les applications figées car elles sont conçues pour interagir avec des périphériques locaux. Les disques durs USB très volumineux peuvent prendre plusieurs minutes pour apparaître dans Windows Explorer.
- Le chargement des cartes flash USB formatées avec le système de fichiers FAT32 est lent. Reportez-vous à la section http://kb.vmware.com/kb/1022836.
- Un processus ou un service sur le système local a ouvert le périphérique avant votre connexion au poste de travail distant.

- Un périphérique USB redirigé arrête de fonctionner si vous reconnectez une session de poste de travail, même si le poste de travail indique que le périphérique est disponible.
- La redirection USB est désactivée dans View Administrator.
- Des pilotes de redirection USB sont manquants ou désactivés sur le client.
- Pour View Client à partir de View 5,0.x ou antérieur, des pilotes sont manquants ou désactivés pour le périphérique redirigé sur le client. View Client à partir de View 5,0.x ou antérieur requiert que vous installiez le pilote USB pour un périphérique redirigé sur le client. View Client depuis la version View 5.1 et les version suivantes n'a pas cette exigence.

Solution

- Si le protocole PCoIP est disponible, utilisez-le à la place de RDP comme protocole de poste de travail.
- Si un périphérique redirigé reste indisponible ou arrête de fonctionner après une déconnexion temporaire, éjectez le périphérique, rebranchez-le et tenter de nouveau l'opération de redirection.
- Dans View Administrator, allez dans **[Règles] > [Règles générales]** et vérifiez que l'accès USB est défini sur **[Allow (Autoriser)]** sous View Policies (Règles de View).
- Recherchez les entrées de classe `wssm_usb` dans le journal sur l'invité et les entrées de classe `wswc_usb` dans le journal sur le client.

  Les entrées avec ces classes sont inscrites dans les journaux si un utilisateur n'est pas un administrateur, ou si les pilotes de redirection USB ne sont pas installés ou ne fonctionnent pas.
- Ouvrez le Gestionnaire de périphériques sur l'invité, développez les contrôleurs USB (Universal Serial Bus) et réinstallez les pilotes VMware View Virtual USB Host Controller et VMware View Virtual USB Hub s'ils manquent ou réactivez-les s'ils sont désactivés.

Dépannage de postes de travail qui sont supprimés et recréés plusieurs fois

View Manager peut supprimer et recréer plusieurs fois des postes de travail de clone lié et de clone complet avec l'état d'erreur.

Problème

Un poste de travail de clone lié ou de clone complet est créé avec un état d'erreur, supprimé et recréé avec un état d'erreur. Ce cycle se répète sans cesse.

Cause

Lorsqu'un pool de postes de travail important est approvisionné, une ou plusieurs machines virtuelles peuvent finir avec un état d'erreur. Le mécanisme de récupération automatique de View Manager tente d'activer la machine virtuelle échouée. Si la machine virtuelle ne s'active pas après un certain nombre de tentatives, View Manager la supprime.

En suivant les exigences de taille de pool, View Manager crée un nouvelle machine virtuelle, souvent avec le même nom de poste de travail que le poste de travail d'origine. Si la nouvelle machine virtuelle est approvisionnée avec la même erreur, elle est supprimée et le cycle se répète.

La récupération automatique est exécutée sur des postes de travail de clone lié et de clone complet.

Si les tentatives de récupération automatique échouent pour une machine virtuelle, View Manager supprime la machine virtuelle uniquement s'il s'agit d'un poste de travail flottant ou d'un poste de travail dédié non affecté à un utilisateur. De plus, View Manager ne supprime pas les machines virtuelles lorsque l'approvisionnement de pool est désactivé.

Solution

Examinez la machine virtuelle parente ou le modèle qui a été utilisé pour créer le pool de postes de travail. Recherchez les erreurs dans la machine virtuelle ou le système d'exploitation client qui peuvent causer l'erreur dans la machine virtuelle.

Pour les clones liés, résolvez les erreurs dans la machine virtuelle parente et prenez un nouveau snapshot.

- Si de nombreux postes de travail ont un état d'erreur, utilisez le nouveau snapshot ou modèle pour recréer le pool.
- Si la plupart des postes de travail sont intègres, sélectionnez le pool de postes de travail dans View Administrator, cliquez sur **[Modifier]** , sélectionnez l'onglet Paramètres de vCenter, sélectionnez le nouveau snapshot comme image de base par défaut et enregistrez vos modifications.

  Les nouveaux postes de travail de clone lié sont créés à l'aide du nouveau snapshot.

Pour les clones complets, résolvez les erreurs dans la machine virtuelle, générez un nouveau modèle et recréez le pool.

Résolution de problèmes de personnalisation de QuickPrep

Un script de personnalisation QuickPrep de View Composer peut échouer pour plusieurs raisons.

Problème

Un script de post-synchronisation ou de désactivation QuickPrep ne s'exécute pas. Dans certains cas, un script peut s'exécuter correctement sur certains clones liés et échouer sur d'autres.

Cause

Quelques causes communes existes pour les problèmes de script QuickPrep :

- Le script expire.
- Le chemin du script fait référence à un script qui requiert un interprète.
- Le compte sous lequel le script s'exécute ne dispose pas d'autorisations suffisantes pour exécuter une tâche de script.

Solution

- Examinez le journal du script de personnalisation.

  Les informations de personnalisation QuickPrep sont inscrites dans un fichier journal dans le répertoire `temp` de Windows :

  ```
  C:\Windows\Temp\vmware-viewcomposer-ga-new.log
  ```

- Déterminez si le script est expiré.

  View Composer termine un script de personnalisation qui dure plus de 20 secondes. Le fichier journal affiche un message indiquant que le script a démarré et un autre message indiquant l'expiration :

  ```
  2010-02-21 21:05:47,687 [1500] INFO Ready -
  [Ready.cpp, 102] Running the PostSync script: cmd /c
  C:\temp\build\composer.bat
  2010-02-21 21:06:07,348 [1500] FATAL Guest -
  [Guest.cpp, 428] script cmd /c
  C:\temp\build\composer.bat timed out
  ```

  Pour résoudre un problème d'expiration, augmentez la limite d'expiration pour le script et exécutez-le de nouveau.

- Déterminez si le chemin du script est valide.

  Si vous utilisez un langage de script qui a besoin d'un interprète pour exécuter le script, le chemin du script doit démarrer par le binaire de l'interprète.

  Par exemple, si vous spécifiez le chemin d'accès `C:\script\myvb.vbs` en tant que script de personnalisation QuickPrep, View Composer Agent ne peut pas exécuter le script. Vous devez spécifier un chemin qui démarre par le chemin du binaire de l'interprète :

  ```
  C:\windows\system32\cscript.exe c:\script\myvb.vbs
  ```

- Déterminez si le compte sous lequel le script s'exécute dispose d'autorisations appropriées pour effectuer des tâches de script.

  QuickPrep exécute les scripts sous le compte dans lequel le service VMware View Composer Guest Agent Server est configuré pour être exécuté. Par défaut, ce compte est `système local`.

  Ne modifiez pas ce compte d'ouverture de session. Si vous le faites, les clones liés ne démarrent pas.

Erreurs d'approvisionnement de View Composer

Si une erreur se produit lorsque View Composer approvisionne ou recompose des postes de travail de clone lié, un code d'erreur indique la cause de l'échec. Le code d'erreur apparaît dans la colonne d'état du poste de travail dans View Administrator.

Tableau 16-2 décrit les codes d'erreur d'approvisionnement de View Composer.

Ce tableau répertorie les erreurs associées à View Composer et à la personnalisation de QuickPrep. Des erreurs supplémentaires peuvent se produire dans View Connection Server et d'autres composants View qui peuvent interférer avec l'approvisionnement de poste de travail.

Tableau 16-2. Erreurs d'approvisionnement de View Composer

Error (Erreur)	Description
0	La règle a été appliquée correctement. **Remarque** Le code de résultat 0 n'apparaît pas dans View Administrator. Le poste de travail de clone lié passe à l'état Ready (Prêt), sauf si une erreur de View Manager en dehors du domaine View Composer se produit. Ce code de résultat est inclus pour couvrir tous les cas de figure.
1	Échec de définition du nom de l'ordinateur.
2	Échec de redirection des profils d'utilisateur vers le disque persistant de View Composer.
3	Échec de définition du mot de passe du compte de domaine de l'ordinateur.
4	Échec de sauvegarde des clés de profil d'un utilisateur. La prochaine fois que l'utilisateur ouvre une session sur ce poste de travail de clone lié après l'opération de recomposition, le système d'exploitation crée un nouveau répertoire de profil pour l'utilisateur. Lors de la création d'un nouveau profil, l'utilisateur ne peut pas voir les anciennes données de profil.
5	Échec de restauration du profil d'un utilisateur. L'utilisateur ne doit pas ouvrir de session sur le poste de travail dans cet état car l'état de profil n'est pas défini.

Tableau 16-2. Erreurs d'approvisionnement de View Composer (suite)

Error (Erreur)	Description
6	Erreurs non couvertes par d'autres codes d'erreur. Les fichiers journaux d'agent de View Composer dans le système d'exploitation client peuvent fournir plus d'informations sur les causes de ces erreurs. Par exemple, un délai d'expiration de Windows Plug-and-Play (PnP) peut générer ce code d'erreur. Dans cette situation, View Composer expire après avoir attendu que le service PnP installe de nouveaux volumes pour la machine virtuelle de clone lié. PnP monte jusqu'à trois disques, en fonction de la configuration du pool : ■ Disque persistant de View Composer ■ Disque non persistant pour rediriger des fichiers temporaires et d'échange du système d'exploitation client ■ Disque interne qui stocke des données de configuration QuickPrep et d'autres données liées au système d'exploitation. Ce disque est toujours configuré avec un clone lié. Le délai d'expiration est de 10 minutes. Si PnP ne termine pas le montage des disques en 10 minutes, View Composer échoue avec le code d'erreur 6.
7	Trop de disques persistants de View Composer sont attachés au clone lié. Un clone peut avoir au plus trois disques persistants de View Composer.
8	Un disque persistant ne peut pas être monté sur le magasin de données sélectionné lors de la création du pool.
9	View Composer ne peut pas rediriger des fichiers de données supprimables vers le disque non persistant. Le fichier d'échange ou les dossiers de fichiers temporaires n'étaient pas redirigés.
10	View Composer ne peut pas trouver le fichier de règle de configuration QuickPrep sur le disque interne spécifié.
12	View Composer ne peut pas trouver le disque interne qui contient le fichier de règle de configuration QuickPrep et d'autres données liées au système d'exploitation.
13	Plusieurs disques persistants sont configurés pour rediriger le profil d'utilisateur Windows.
14	View Composer n'a pas réussi à démonter le disque interne.
15	Le nom d'ordinateur que View Composer a lu depuis le fichier de règle de configuration ne correspond pas au nom du système actuel après la première mise sous tension du clone lié.
16	L'agent View Composer n'a pas démarré car la licence en volume pour le système d'exploitation client n'était pas activée.
17	L'agent View Composer n'a pas démarré. L'agent a expiré en attendant que Sysprep démarre.
18	L'agent View Composer n'a pas pu joindre la machine virtuelle de clone lié au domaine lors de la personnalisation.
19	L'agent View Composer n'a pas pu exécuter un script de post-synchronisation.
20	L'agent View Composer n'a pas pu gérer un événement de synchronisation de mot de passe de machine. Cette erreur peut être temporaire. Si le clone lié joint le domaine, le mot de passe est correct. Si le clone ne parvient pas à joindre le domaine, redémarrez l'opération que vous avez effectuée avant que l'erreur se produise. Si vous avez redémarré le clone, redémarrez-le de nouveau. Si vous avez actualisé le clone, actualisez-le de nouveau. Si le clone ne parvient toujours pas à joindre le domaine, recomposez le clone.

Retrait des clones liés orphelins ou supprimés

Dans certaines conditions, les données de clone lié dans View, View Composer et vCenter Server peuvent être désynchronisées et vous pouvez ne pas être capable d'approvisionner ou de supprimer des postes de travail de clone lié.

Problème

- Vous ne pouvez pas approvisionner un pool de postes de travail de clone lié.

- L'approvisionnement de postes de travail de clone lié échoue et l'erreur suivante se produit : `La machine virtuelle avec la spécification entrée existe déjà`
- Dans View Administrator, les postes de travail de clone lié sont bloqués dans un état `Deleting`. Vous ne pouvez pas redémarrer la commande Supprimer dans View Administrator car les postes de travail sont déjà dans l'état `Deleting`.

Cause

Ce problème se produit si la base de données View Composer contient des informations sur les clones liés qui sont incohérentes avec les informations dans View LDAP, Active Directory ou vCenter Server. Plusieurs situations peuvent provoquer cette incohérence :

- Le nom de la machine virtuelle de clone lié est modifié manuellement dans vCenter Server après la création du pool, ce qui entraîne View Composer et vCenter Server à se reporter à la même machine virtuelle avec des noms différents.
- Un échec de stockage ou une opération manuelle provoque la suppression de la machine virtuelle de vCenter Server. Les données du poste de travail de clone lié existent toujours dans la base de données View Composer, View LDAP et Active Directory.
- Pendant qu'un pool est supprimé de View Administrator, un échec de réseau ou autre laisse la machine virtuelle dans vCenter Server.

Solution

Si la machine virtuelle a été renommée dans vSphere Client après l'approvisionnement du pool de postes de travail, essayez de renommer la machine virtuelle avec le nom qui était utilisé lorsqu'elle a été déployée dans View.

Si d'autres informations sur la base de données sont incohérentes, utilisez la commande `SviConfig RemoveSviClone` pour supprimer ces éléments :

- Les entrées de base de données de clone lié de la base de données View Composer
- Le compte de machine de clone lié d'Active Directory
- La machine virtuelle de clone lié de vCenter Server

L'utilitaire `SviConfig` se trouve sur l'ordinateur sur lequel View Composer est installé dans l'emplacement suivant :

- Ordinateurs 32 bits : *`Install_drive`*`\Program Files\VMware\VMware View Composer`
- Ordinateurs 64 bits : *`Install_drive`*`\Program Files (x86)\VMware\VMware View Composer`

IMPORTANT Seuls les administrateurs View Composer expérimentés doivent utiliser l'utilitaire `SviConfig`. Cet utilitaire est conçu pour résoudre des problèmes liés au service View Composer.

Procédez comme suit :

1 Vérifiez que le service View Composer est en cours d'exécution.

2 À partir d'une invite de commande Windows sur l'ordinateur View Composer, exécutez la commande `SviConfig RemoveSviClone` au format suivant :

```
sviconfig –operation=removesviclone
          –VmName=virtual machine name
          [–AdminUser=local administrator username]
          –AdminPassword=local administrator password
          [–ServerUrl=View Composer server URL]
```

Par exemple :

```
sviconfig –operation=removesviclone –vmname=MyLinkedClone
 –adminuser=Admin –adminpassword=Pass –serverurl=ViewComposerURL
```

Les paramètres `VmName` et `AdminPassword` sont requis. La valeur par défaut du paramètre `AdminUser` est `Administrator`. La valeur par défaut du paramètre `ServerURL` est `https://localhost:18443/SviService/v2_0`

Pour plus d'informations sur la suppression des informations de machine virtuelle de View LDAP, consultez l'article 2015112 de la base de connaissances VMware : *Manually deleting linked clones or stale virtual desktop entries from VMware View Manager 4.5 and later (Supprimer manuellement des clones liés ou des entrées de poste de travail virtuel périmées de VMware View Manager 4.5 et supérieur).*

Recherche et suppression de la protection des réplicas View Composer inutilisés

Dans certains cas, les réplicas View Composer peuvent rester dans vCenter Server lorsqu'ils n'ont plus de clones liés associés.

Problème

Un réplica inutilisé reste dans un dossier vCenter Server. Vous ne pouvez pas supprimer le réplica en utilisant vSphere Client.

Cause

Les indisponibilités de réseau au cours des opérations View Composer ou de la suppression des clones liés associés directement depuis vSphere sans utiliser les commandes View appropriées, peut laisser un réplica inutilisé dans vCenter Server.

Les réplicas sont des entités protégées dans vCenter Server. Ils ne peuvent pas être supprimés avec les commandes de gestion ordinaires de vCenter Server ou de vSphere Client.

Solution

Utilisez la commande `SviConfig FindUnusedReplica` pour rechercher le réplica dans un dossier donné. Vous pouvez utiliser le paramètre `–Move` pour transférer le réplica vers un autre dossier. Le paramètre `–Move` lève la protection d'un réplica inutilisé avant de le déplacer.

IMPORTANT Seuls les administrateurs expérimentés de View Composer doivent utiliser l'utilitaire `SviConfig`. Cet utilitaire est conçu pour résoudre des problèmes liés au service View Composer.

L'utilitaire `SviConfig` se trouve dans l'emplacement suivant sur l'ordinateur sur lequel View Composer est installé :

- Ordinateurs 32 bits : *`Install_drive`*`\Program Files\VMware\VMware View Composer`
- Ordinateurs 64 bits : *`Install_drive`*`\Program Files (x86)\VMware\VMware View Composer`

Avant de commencer, vérifiez qu'aucun clone lié n'est associé au réplica.

Familiarisez-vous avec les paramètres `SviConfig FindUnusedReplica` :

- `DsnName`. DSN qui doit être utilisé pour se connecter à la base de données.
- `UserName`. Nom d'utilisateur utilisé pour se connecter à la base de données. Si vous ne définissez pas ce paramètre, l'authentification Windows est utilisée.
- `Password (Mot de passe)`. Mot de passe de l'utilisateur qui se connecte à la base de données. Si vous ne définissez pas ce paramètre et que l'authentification Windows n'est pas utilisée, un message demande ensuite d'entrer le mot de passe.

- `ReplicaFolder`. Nom du dossier de réplica. Utilisez une chaîne vide pour le dossier racine. La valeur par défaut est `VMwareViewComposerReplicaFolder`.
- `UnusedReplicaFolder`. Nom du dossier devant contenir tous les réplicas inutilisés. La valeur par défaut est `UnusedViewComposerReplicaFolder`. Utilisez ce paramètre pour définir le dossier de destination lorsque vous utilisez le paramètre `Move`.
- `OutputDir`. Nom du répertoire de sortie dans lequel la liste des réplicas inutilisés stockés dans le fichier `unused-replica-*.txt` est générée. La valeur par défaut est le répertoire de travail en cours.
- `Move`. Détermine s'il est nécessaire de lever la protection des machines virtuelles de réplica inutilisés et de les transférer vers un dossier défini. Le paramètre `UnusedReplicaFolder` spécifie le dossier de destination. La valeur par défaut du paramètre `Move` est `false`.

Les paramètres `DsnName`, `Username` et `Password` sont obligatoires. `DsnName` ne peut pas être une chaîne vide.

Effectuez ces étapes :

1 Redémarrez le service View Composer.

2 Dans une invite de commande Windows sur l'ordinateur de View Composer, exécutez la commande `SviConfig FindUnusedReplica` suivante :

```
sviconfig -operation=findunusedreplica
         -DsnName=name of the DSN
         -Username=Database administrator username
         -Password=Database administrator password
         [-ReplicaFolder=Replica folder name]
         [-UnusedReplicaFolder=Unused replica folder name.]
         [-OutputDir=Output file directory]
         [-Move=true or false]
```

Par exemple :

```
sviconfig -operation=FindUnusedReplica -DsnName=SVI
  -Username=SVIUser -Password=1234 -Move=True
```

3 Redémarrez le service View Composer.

4 (Facultatif) Une fois le réplica transféré vers le nouveau dossier, supprimez la machine virtuelle de réplica de vCenter Server.

Les clones liés Windows XP ne parviennent pas à joindre le domaine

Les postes de travail de clone lié Windows XP peut ne pas parvenir à joindre le domaine si votre Active Directory s'exécute sur Windows Server 2008.

Problème

Lorsque des postes de travail de clone lié sont approvisionnés, les clones liés ne parviennent pas à joindre le domaine. View Administrator affiche des messages d'erreur d'approvisionnement de View Composer. Par exemple :

```
5/17/10 3:11:50 PM PDT: View Composer agent initialization state error (18): Failed to join the
domain (waited 565 seconds) (5/17/10 3:11:50 PM PDT : erreur d'état d'initialisation de l'agent
View Composer (18) : impossible de joindre le domaine (attendu 565 secondes))
```

Cause

Ce problème peut se produire si votre Active Directory s'exécute sur Windows Server 2008. La compatibilité descendante du contrôleur de domaine en lecture seule Windows Server 2008 (RODC) avec des machines virtuelles Windows XP n'est pas possible.

Solution

1 Recherchez dans le journal de View Composer le message d'erreur suivant :

`0x4f1: The system detected a possible attempt to compromise security. Please ensure that you can contact the server that authenticated you. (0x4f1 : le système a détecté une tentative possible de compromission de la sécurité. Vérifiez que vous pouvez contacter le serveur qui vous a authentifié.)`

Par défaut, le fichier journal de View Composer est généré dans le répertoire `Temp` de Windows : `C:\Windows\Temp\vmware-viewcomposer-ga-new.log`

2 Sur la machine virtuelle parente, appliquez la mise à jour de compatibilité du contrôleur de domaine en lecture seule Windows Server 2008 pour Windows XP.

Consultez l'article 944043 du support Microsoft à l'adresse suivante : http://support.microsoft.com/kb/944043/en-us.

3 Prenez un snapshot de la machine virtuelle parente mise à jour.

4 Recomposez les postes de travail de clone lié à partir de la machine virtuelle parente mise à jour et du snapshot.

Résolution des problèmes GINA sur des postes de travail Windows XP

Sur les postes de travail Windows XP, des problèmes peuvent se produire avec le chaînage des fichiers de bibliothèque de liens dynamiques (dll) GINA (Graphical Identification and Authentication) de VMware View.

Problème

Les problèmes suivants peuvent se produire sur des postes de travail Windows XP :

- Un poste de travail ne démarre pas
- Lorsqu'un poste de travail démarre ou s'arrête, l'erreur suivante est affichée : `Cannot start gina.dll module. A required component is missing: gina.dll. Please install the application again. (Impossible de démarrer le module gina.dll. Un composant requis est manquant : gina.dll. Veuillez installer de nouveau l'application.)`
- Lorsque vous démarrez un poste de travail, une invite d'ouverture de session inattendue apparaît
- Vous ne pouvez pas ouvrir de session sur votre poste de travail

Cause

Des problèmes de démarrage et d'ouverture de session peuvent se produire sur des postes de travail Windows XP lorsque les fichiers `dll` GINA de View ne sont pas chaînés correctement avec des GINA tiers qui peuvent résider sur les machines virtuelles.

Pour vous assurer que le GINA est chaîné correctement, vous devez configurer le GINA `WinLogon` pour qu'il s'agisse du GINA View et vous assurer que le fichier `vdmGinaChainDLL` est créé et qu'il contient les GINA tiers.

Si vous n'avez pas installé de logiciel qui chaîne vers un GINA différent, le fichier par défaut est `msgina.dll`, qui se trouve à `%systemroot%\system32\msgina.dll` sur la machine virtuelle.

Solution

1 Ouvrez une session sur la machine virtuelle parente, la machine virtuelle modèle ou le poste de travail View.

2 Cliquez sur **[Start (Démarrer)] > [Run (Exécuter)]** , saisissez **`Regedit`** et appuyez sur Enter (Entrée).

3 Recherchez la clé de Registre Windows suivante :

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\Current Version\Winlogon\GinaDLL`

4 Assurez-vous que la clé `GinaDLL` possède la valeur suivante :

install_directory\VMware\VMware View\Agent\bin\wsgina.dll

install_directory est le chemin où vous avez installé View Agent.

5 Si la valeur de chaîne `vdmGinaChainDLL` n'existe pas, créez-la.

a Recherchez la clé de Registre suivante :

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\Current Version`

b Créez la clé `vdmGinaChainDLL`.

6 Placez les noms `dll` GINA tiers dans la clé `vdmGinaChainDLL`.

7 Si vous rencontrez toujours des problèmes avec les postes de travail Windows XP, assurez-vous qu'aucune clé GINA spécifique du fournisseur n'est chargée dans le Registre.

Si des clés GINA tierces sont chargées, le GINA de chaînage peut toujours appeler le GINA par défaut, `msgina`. Certains produits de gestion de réseau et de logiciel de sécurité placent leurs fichiers `dlls` de remplacement GINA dans leurs propres répertoires d'installation, dans des chemins de Registre tels que le suivant :

`HKEY_LOCAL_MACHINE\Software\`*`Vendor_ID_or_Name`*`\`*`GINA_key_reference`*`\`*`GINA_Load_Instruction`* `= msgina`

Supprimez ces clés GINA de l'emplacement spécifique du fournisseur et placez-les dans la clé `vdmGinaChainDLL`.

Autres informations de dépannage

Vous pouvez trouver davantage d'informations de dépannage dans des articles de la base de connaissances VMware.

La base de connaissances VMware est mise à jour en continu avec des nouvelles informations de dépannage pour des produits VMware.

Pour plus d'informations sur le dépannage de View Manager, consultez les articles de la base de connaissances disponibles sur le site Web de la base de connaissances VMware :

http://kb.vmware.com/selfservice/microsites/microsite.do

Utilisation de la commande vdmadmin 17

Vous pouvez utiliser l'interface de ligne de commande `vdmadmin` pour effectuer diverses tâches d'administration sur une instance de Serveur de connexion View.

Vous pouvez utiliser `vdmadmin` pour effectuer des tâches d'administration qui ne sont pas possibles dans l'interface utilisateur de View Administrator ou pour effectuer des tâches d'administration qui doivent s'exécuter automatiquement depuis des scripts.

Pour voir une comparaison des opérations qui sont possibles dans View Administrator, des cmdlets View et `vdmadmin`, consultez le document *Intégration de VMware Horizon View*.

- Génération de messages de journal des événements View au format Syslog à l'aide de l'option -I page 474

  Vous pouvez utiliser la commande `vdmadmin` avec l'option `–I` pour enregistrer des messages d'événement View au format `Syslog` dans des fichiers de journal des événements. De nombreux produits d'analyse tiers requièrent des données `Syslog` de fichier plat comme entrée pour leurs opérations d'analyse.

- Affectation de postes de travail dédiés à l'aide de l'option -L page 475

  Vous pouvez utiliser la commande `vdmadmin` avec l'option `–L` pour affecter des postes de travail d'un pool dédié à des utilisateurs.

- Affichage d'informations sur les machines à l'aide de l'option -M page 476

  Vous pouvez utiliser la commande `vdmadmin` avec l'option `–M` pour afficher des informations sur la configuration de machines virtuelles ou d'ordinateurs physiques.

- Récupération d'espace disque sur des machines virtuelles à l'aide de l'option -M page 478

  Vous pouvez utiliser la commande `vdmadmin` avec l'option `–M` pour marquer une machine virtuelle de clone lié pour la récupération d'espace disque. View demande à l'hôte ESXi de récupérer l'espace disque sur le disque du système d'exploitation de clone lié sans attendre que l'espace inutilisé sur le disque du système d'exploitation atteigne le seuil minimal spécifié dans View Administrator.

- Configuration de filtres de domaine à l'aide de l'option -N page 479

  Vous pouvez utiliser la commande `vdmadmin` avec l'option `–N` pour contrôler les domaines que View Manager rend disponibles pour les utilisateurs finaux.

- Configuration de filtres de domaine page 481

  Vous pouvez configurer des filtres de domaine pour limiter les domaines qu'une instance de View Connection Server ou un serveur de sécurité rend disponibles aux utilisateurs finaux.

- Affichage des postes de travail et des règles d'utilisateurs non autorisés à l'aide des options -O et -P page 485

  Vous pouvez utiliser la commande `vdmadmin` avec les options `–O` et `–P` pour afficher les postes de travail et les règles affectés à des utilisateurs qui ne sont plus autorisés à utiliser le système.

- Configuration de clients en mode kiosque à l'aide de l'option -Q page 487

  Vous pouvez utiliser la commande `vdmadmin` avec l'option `–Q` pour définir des valeurs par défaut et créer des comptes pour des clients en mode kiosque, pour activer l'authentification pour ces clients et pour afficher des informations sur leur configuration.

- Affichage du premier utilisateur d'un poste de travail à l'aide de l'option -R page 491

  Vous pouvez utiliser la commande `vdmadmin` avec l'option `–R` pour en savoir plus sur l'affectation initiale d'un poste de travail géré. Par exemple, en cas de perte de données LDAP, vous pouvez avoir besoin de ces informations pour pouvoir affecter de nouveau des postes de travail à des utilisateurs.

- Suppression de l'entrée pour une instance de Serveur de connexion View ou un serveur de sécurité à l'aide de l'option -S page 491

  Vous pouvez utiliser la commande `vdmadmin` avec l'option `–S` pour supprimer l'entrée d'une instance de Serveur de connexion View ou d'un serveur de sécurité depuis la configuration de View Manager.

- Définition de la limite de division pour la publication de packages View Transfer Server à l'aide de l'option -T page 492

  Vous pouvez utiliser la commande `vdmadmin` avec l'option `–T` pour définir la limite de division pour la publication de packages View Transfer Server. Vous voulez peut-être spécifier une limite de division si vous utilisez un cache proxy qui définit une taille d'objet maximale pour son cache.

- Affichage d'informations sur les utilisateurs à l'aide de l'option -U page 493

  Vous pouvez utiliser la commande `vdmadmin` avec l'option `–U` pour afficher des informations détaillées sur les utilisateurs.

- Décryptage de la machine virtuelle d'un poste de travail local à l'aide de l'option -V page 493

  Présentation sécurise la machine virtuelle d'un poste de travail local en cryptant son image de base. Si vous ne parvenez pas à alimenter ou à restituer le poste de travail local, vous pouvez utiliser la commande `vdmadmin` avec l'option `–V` pour décrypter la machine virtuelle de façon à en restaurer certaines données.

- Récupération d'un poste de travail en utilisant l'option -V lorsque le poste de travail a été modifié dans le datacenter page 494

  Lorsqu'une opération en mode local, telle qu'un emprunt, une restitution ou une réplication, est exécutée, View valide le fait que la machine virtuelle du poste de travail View dans vCenter Server n'a pas été modifiée depuis la dernière synchronisation avec le poste de travail local View. Si un disque de machine virtuelle dans vCenter Server a été modifié et que le disque ne corresponde pas à la version du poste de travail local, vous pouvez utiliser la commande `vdmadmin` avec l'option `–V` pour conserver les données sur le poste de travail local et la machine virtuelle vCenter Server et faire en sorte que les deux versions soient synchronisées.

- Déverrouillage ou verrouillage de machines virtuelles à l'aide de l'option -V page 496

  Vous pouvez utiliser la commande `vdmadmin` avec l'option `–V` pour déverrouiller ou verrouiller des machines virtuelles dans le datacenter.

- Détection et résolution des collisions d'entrée LDAP à l'aide de l'option -X page 497

  Vous pouvez utiliser la commande `vdmadmin` avec l'option `–X` pour détecter et résoudre les entrées LDAP en collision sur des instances de View Connection Server répliquées dans un groupe.

Utilisation de la commande vdmadmin

La syntaxe de la commande `vdmadmin` contrôle son fonctionnement.

Utilisez la forme suivante de la commande `vdmadmin` dans une invite de commande Windows.

`vdmadmin` *`command_option`* [*`additional_option argument`*] `...`

Les options supplémentaires que vous pouvez utiliser dépendent de l'option de commande.

Par défaut, le chemin d'accès vers le fichier exécutable de la commande `vdmadmin` est `C:\Program Files\VMware\VMware View\Server\tools\bin`. Pour éviter d'avoir à entrer le chemin sur la ligne de commande, ajoutez le chemin vers votre variable d'environnement *PATH*.

- Authentification de commande vdmadmin page 465

  Vous devez exécuter la commande `vdmadmin` en tant qu'utilisateur qui est dans le rôle **Administrators (Administrateurs)** pour qu'une action spécifiée réussisse.

- Format de sortie de la commande vdmadmin page 466

  Certaines options de la commande `vdmadmin` vous permettent de spécifier le format des informations de sortie.

- Options de la commande vdmadmin page 466

  Vous utilisez les options de commande de la commande `vdmadmin` pour spécifier l'opération que vous voulez qu'elle effectue.

Authentification de commande vdmadmin

Vous devez exécuter la commande `vdmadmin` en tant qu'utilisateur qui est dans le rôle **Administrators (Administrateurs)** pour qu'une action spécifiée réussisse.

Vous pouvez utiliser View Administrator pour affecter le rôle **Administrators (Administrateurs)** à un utilisateur. Pour plus d'informations sur la configuration de connexions directes, reportez-vous à la section Chapitre 2, « Configuration d'administration déléguée basée sur des rôles », page 41.

Si vous avez ouvert une session en tant qu'utilisateur avec des privilèges insuffisants, vous pouvez utiliser l'option –b pour exécuter la commande en tant qu'utilisateur avec le rôle **Administrators (Administrateurs)** à condition que vous connaissiez son mot de passe. Vous pouvez spécifier l'option –b pour exécuter la commande vdmadmin en tant qu'utilisateur spécifié dans le domaine spécifié. Les formes d'utilisation suivantes de l'option –b sont équivalentes.

```
–b username domain [password | *]
–b username@domain [password | *]
–b domain\username [password | *]
```

Si vous spécifiez un astérisque (*) au lieu d'un mot de passe, vous êtes invité à saisir le mot de passe. Vous pouvez utiliser l'option –b avec toutes les options de commande sauf les options –R et –T.

Format de sortie de la commande vdmadmin

Certaines options de la commande vdmadmin vous permettent de spécifier le format des informations de sortie.

Tableau 17-1 montre les options que certaines options de la commande vdmadmin fournissent pour la mise en forme du texte de sortie.

Tableau 17-1. Options pour la sélection du format de sortie

Option	Description
–csv	Met en forme la sortie sous forme de valeurs séparées par des virgules.
–n	Affiche la sortie à l'aide de caractères ASCII (UTF-8). Il s'agit du jeu de caractères par défaut pour la sortie de valeurs séparées par des virgules et de texte brut.
–w	Affiche la sortie à l'aide de caractères Unicode (UTF-16). Il s'agit du jeu de caractères par défaut pour la sortie XML.
–xml	Met en forme la sortie au format XML.

Options de la commande vdmadmin

Vous utilisez les options de commande de la commande vdmadmin pour spécifier l'opération que vous voulez qu'elle effectue.

Tableau 17-2 montre les options de commande que vous pouvez utiliser avec la commande vdmadmin pour contrôler et examiner le fonctionnement de View Manager.

Tableau 17-2. Options de la commande Vdmadmin

Option	Description
–A	Administre les informations que View Agent enregistre dans ses fichiers journaux. Reportez-vous à la section « Configuration de la journalisation dans View Agent à l'aide de l'option -A », page 468. Remplace l'adresse IP signalée par View Agent. Reportez-vous à la section « Remplacement d'adresses IP à l'aide de l'option -A », page 469
–C	Définit le nom d'un groupe View Connection Server. Reportez-vous à la section « Définition du nom d'un groupe Serveur de connexion View à l'aide de l'option -C », page 470.
–F	Met à jour les sécurités extérieures principales (FSP) dans Active Directory pour tous les utilisateurs ou des utilisateurs spécifiques. Reportez-vous à la section « Mise à jour de sécurités extérieures principales à l'aide de l'option -F », page 471.
–H	Affiche des informations sur la santé de services View Manager. Reportez-vous à la section « Liste et affichage de moniteurs d'intégrité à l'aide de l'option -H », page 472.
–I	Génère des rapports sur le fonctionnement de View Manager. Reportez-vous à la section « Liste et affichage de rapports sur le fonctionnement de View Manager à l'aide de l'option -I », page 473.

Tableau 17-2. Options de la commande Vdmadmin (suite)

Option	Description
–L	Affecte un poste de travail dédié à un utilisateur ou supprime une affectation. Reportez-vous à la section « Affectation de postes de travail dédiés à l'aide de l'option -L », page 475.
–M	Affiche des informations sur une machine virtuelle ou un ordinateur physique. Reportez-vous à la section « Affichage d'informations sur les machines à l'aide de l'option -M », page 476.
–N	Configure les domaines qu'une instance de View Connection Server ou un groupe rend disponibles à des clients View Client. Reportez-vous à la section « Configuration de filtres de domaine à l'aide de l'option -N », page 479.
–O	Affiche les postes de travail affectés à des utilisateurs qui ne sont plus autorisés sur ces postes de travail. Reportez-vous à la section « Affichage des postes de travail et des règles d'utilisateurs non autorisés à l'aide des options -O et -P », page 485.
–P	Affiche les règles utilisateur associées aux postes de travail d'utilisateurs non autorisés. Reportez-vous à la section « Affichage des postes de travail et des règles d'utilisateurs non autorisés à l'aide des options -O et -P », page 485.
–Q	Configure le compte dans Active Directory et la configuration de View Manager d'un périphérique client en mode kiosque. Reportez-vous à la section « Configuration de clients en mode kiosque à l'aide de l'option -Q », page 487.
–R	Signale le premier utilisateur qui a accédé à un poste de travail. Reportez-vous à la section « Affichage du premier utilisateur d'un poste de travail à l'aide de l'option -R », page 491.
–S	Supprime une entrée de configuration pour une instance de View Connection Server de la configuration de View Manager. Reportez-vous à la section « Suppression de l'entrée pour une instance de Serveur de connexion View ou un serveur de sécurité à l'aide de l'option -S », page 491.
–T	Définit la limite de division de packages View Transfer Server. Reportez-vous à la section « Définition de la limite de division pour la publication de packages View Transfer Server à l'aide de l'option -T », page 492.
–U	Affiche des informations sur un utilisateur, y compris ses autorisations de poste de travail et ses affectations ThinApp, ainsi que les rôles Administrateur. Reportez-vous à la section « Affichage d'informations sur les utilisateurs à l'aide de l'option -U », page 493.
–V	Permet de restaurer des données à partir d'un poste de travail local en décryptant sa machine virtuelle. Reportez-vous à la section « Décryptage de la machine virtuelle d'un poste de travail local à l'aide de l'option -V », page 493. Déverrouille ou verrouille des machines virtuelles incluant des postes de travail locaux et des instances de View Transfer Server. Reportez-vous à la section « Déverrouillage ou verrouillage de machines virtuelles à l'aide de l'option -V », page 496.
–X	Détecte et résout les entrées LDAP en double dans des instances de View Connection Server répliquées. Reportez-vous à la section « Détection et résolution des collisions d'entrée LDAP à l'aide de l'option -X », page 497.

Configuration de la journalisation dans View Agent à l'aide de l'option -A

Vous pouvez utiliser la commande `vdmadmin` avec l'option –A pour configurer la journalisation par View Agent.

Syntaxe

```
vdmadmin –A [–b authentication_arguments] –getDCT–outfile local_file –d desktop –m machine

vdmadmin –A [–b authentication_arguments] –getlogfile logfile –outfile local_file –d desktop –m machine

vdmadmin –A [–b authentication_arguments] –getloglevel [–xml] –d desktop [–m machine]

vdmadmin –A [–b authentication_arguments] –getstatus [–xml] –d desktop [–m machine]

vdmadmin –A [–b authentication_arguments] –getversion [–xml] –d desktop [–m machine]

vdmadmin –A [–b authentication_arguments] –list [–xml] [–w | –n] –d desktop –m machine

vdmadmin –A [–b authentication_arguments] –setloglevel level –d desktop [–m machine]
```

Notes d'utilisation

Pour aider le support technique de VMware à résoudre les problèmes de View Agent, vous pouvez créer un groupe DCT (Data Collection Tool). Vous pouvez également modifier le niveau de journalisation, afficher la version et l'état de View Agent et enregistrer des fichiers journaux individuels sur votre disque local.

Options

Tableau 17-3 montre les options que vous pouvez spécifier pour configurer la journalisation dans View Agent.

Tableau 17-3. Options pour la configuration de la journalisation dans View Agent

Option	Description
`–d` *desktop*	Spécifie le pool de postes de travail.
`–getDCT`	Crée un groupe DCT (Data Collection Tool) et l'enregistre dans un fichier local.
`–getlogfile` *logfile*	Spécifie le nom du fichier journal pour lequel enregistrer une copie.
`–getloglevel`	Affiche le niveau de journalisation actuel de View Agent.
`–getstatus`	Affiche l'état de View Agent.
`–getversion`	Affiche la version de View Agent.
`–list`	Répertorie les fichiers journaux pour View Agent.
`–m` *machine*	Spécifie la machine dans un pool de postes de travail.

Tableau 17-3. Options pour la configuration de la journalisation dans View Agent (suite)

Option	Description	
`–outfile` *local_file*	Spécifie le nom du fichier local dans lequel enregistrer un groupe DCT ou une copie d'un fichier journal.	
`–setloglevel` *level*	Définit le niveau de journalisation de View Agent.	
	debug	Journalise les événements d'erreur, d'avertissement et de débogage.
	normal	Journalise les événements d'erreur et d'avertissement.
	trace	Journalise les événements d'erreur, d'avertissement, informatifs et de débogage.

Exemples

Affichez le niveau de journalisation de Agent pour la machine machine1 dans le pool de postes de travail dtpool2.

```
vdmadmin –A –d dtpool2 –m machine1 –getloglevel
```

Définissez le niveau de journalisation de View Agent pour la machine machine1 dans le pool de postes de travail dtpool2 à déboguer.

```
vdmadmin –A –d dtpool2 –m machine1 –setloglevel debug
```

Affichez la liste de fichiers journaux de View Agent pour la machine machine1 dans le pool de postes de travail dtpool2.

```
vdmadmin –A –d dtpool2 –m machine1 –list
```

Enregistrez une copie du fichier journal View Agent `log–2009–01–02.txt` pour la machine machine1 dans le pool de postes de travail dtpool2 avec le nom `C:\mycopiedlog.txt`.

```
vdmadmin –A –d dtpool2 –m machine1 –getlogfile log–2009–01–02.txt –outfile C:\mycopiedlog.txt
```

Affichez la version de View Agent pour la machine machine1 dans le pool de postes de travail dtpool2.

```
vdmadmin –A –d dtpool2 –m machine1 –getversion
```

Affichez l'état de View Agent pour la machine machine1 dans le pool de postes de travail dtpool2.

```
vdmadmin –A –d dtpool2 –m machine1 –getstatus
```

Créez le groupe DCT pour la machine machine1 dans le pool de postes de travail dtpool2 et inscrivez-le dans le fichier zip `C:\myfile.zip`.

```
vdmadmin –A –d dtpool2 –m machine1 –getDCT –outfile C:\myfile.zip
```

Remplacement d'adresses IP à l'aide de l'option -A

Vous pouvez utiliser la commande `vdmadmin` avec l'option `–A` pour remplacer l'adresse IP signalée par View Agent.

Syntaxe

```
vdmadmin –A [–b authentication_arguments] –override –i ip_or_dns –d desktop –m machine
```

```
vdmadmin –A [–b authentication_arguments] –override –list –d desktop –m machine
```

```
vdmadmin –A [–b authentication_arguments] –override –r –d desktop [–m machine]
```

Notes d'utilisation

View Agent signale l'adresse IP découverte de la machine sur laquelle il est exécuté à l'instance de View Connection Server. Dans des configurations sécurisées où l'instance de View Connection Server ne peut pas approuver la valeur signalée par View Agent, vous pouvez remplacer la valeur fournie par View Agent et spécifier l'adresse IP que la machine gérée devrait utiliser. Si l'adresse d'une machine signalée par View Agent ne correspond pas à l'adresse définie, vous ne pouvez pas utiliser un client View pour accéder à la machine.

Options

Tableau 17-4 montre les options que vous pouvez spécifier pour remplacer des adresses IP.

Tableau 17-4. Options pour le remplacement d'adresses IP

Option	Description
`–d` *desktop*	Spécifie le pool de postes de travail.
`–i` *ip_or_dns*	Spécifie l'adresse IP ou le nom de domaine résolvable dans DNS.
`–m` *machine*	Spécifie le nom de la machine dans un pool de postes de travail.
`–override`	Spécifie une opération pour le remplacement des adresses IP.
`–r`	Supprime une adresse IP remplacée.

Exemples

Remplacez l'adresse IP de remplacement pour la machine machine2 dans le pool de postes de travail dtpool2.

```
vdmadmin –A –override –i 10.20.54.165 –d dtpool2 –m machine2
```

Affichez les adresses IP définies pour la machine machine2 dans le pool de postes de travail dtpool2.

```
vdmadmin –A –override –list –d dtpool2 –m machine2
```

Supprimez les adresses IP définies pour la machine machine2 dans le pool de postes de travail dtpool2.

```
vdmadmin –A –override –r –d dtpool2 –m machine2
```

Supprimez les adresses IP définies pour les postes de travail dans le pool de postes de travail dtpool3.

```
vdmadmin –A –override –r –d dtpool3
```

Définition du nom d'un groupe Serveur de connexion View à l'aide de l'option -C

Vous pouvez utiliser la commande `vdmadmin` avec l'option `–C` pour définir le nom d'un groupe Serveur de connexion View. La console Microsoft SCOM (System Center Operations Manager) affiche ce nom pour vous aider à identifier le groupe dans SCOM.

Syntaxe

```
vdmadmin –C [–b authentication_arguments] [–c groupname]
```

Notes d'utilisation

Vous devez nommer un groupe Serveur de connexion View si vous prévoyez d'utiliser SCOM pour surveiller et gérer l'état de composants View Manager. View Administrator n'affiche pas le nom d'un groupe. Exécutez la commande sur un membre du groupe que vous voulez nommer.

Si vous ne spécifiez pas de nom pour le groupe, la commande renvoie le GUID du groupe auquel l'instance locale de Serveur de connexion View appartient. Vous pouvez utiliser le GUID pour vérifier si une instance de Serveur de connexion View est un membre du même groupe Serveur de connexion View qu'une autre instance de Serveur de connexion View.

Pour voir une description de l'utilisation de SCOM avec View, consultez le document *Intégration de VMware Horizon View*.

Options

L'option `-c` spécifie le nom du groupe Serveur de connexion View. Si vous ne spécifiez pas cette option, la commande renvoie le GUID du groupe.

Exemples

Définissez le nom d'un groupe Serveur de connexion View sur VCSG01.

```
vdmadmin -C -c VCSG01
```

Renvoyez le GUID du groupe.

```
vdmadmin -C
```

Mise à jour de sécurités extérieures principales à l'aide de l'option -F

Vous pouvez utiliser la commande `vdmadmin` avec l'option `-F` pour mettre à jour les sécurités extérieures principales (FSP) d'utilisateurs Windows dans Active Directory autorisés à utiliser un poste de travail.

Syntaxe

```
vdmadmin -F [-b authentication_arguments] [-u domain\user]
```

Notes d'utilisation

Si vous approuvez des domaines en dehors de vos domaines locaux, vous autorisez l'accès par des sécurités principales dans les domaines externes sur les ressources des domaines locaux. Active Directory utilise des FSP pour représenter des sécurités principales dans des domaines externes approuvés. Vous voulez peut-être mettre à jour les FSP d'utilisateurs si vous modifiez la liste de domaines externes approuvés.

Options

L'option `-u` spécifie le nom et le domaine de l'utilisateur pour lequel vous voulez mettre à jour la FSP. Si vous ne spécifiez pas cette option, la commande met à jour les FSP de tous les utilisateurs dans Active Directory.

Exemples

Mettez à jour la FSP de l'utilisateur Jim dans le domaine EXTERNAL.

```
vdmadmin -F -u EXTERNAL\Jim
```

Mettez à jour les FSP de tous les utilisateurs dans Active Directory.

```
vdmadmin -F
```

Liste et affichage de moniteurs d'intégrité à l'aide de l'option -H

Vous pouvez utiliser la commande `vdmadmin` avec l'option `–H` pour répertorier les moniteurs d'intégrité et les instances de contrôle existants des composants View Manager, et pour afficher les détails d'un moniteur d'intégrité ou d'une instance de contrôle spécifique.

Syntaxe

```
vdmadmin –H [–b authentication_arguments] –list –xml [–w | –n]
```

```
vdmadmin –H [–b authentication_arguments] –list –monitorid monitor_id –xml [–w | –n]
```

```
vdmadmin –H [–b authentication_arguments] –monitorid monitor_id –instanceid instance_id –xml [–w | –n]
```

Notes d'utilisation

Tableau 17-5 indique les moniteurs d'intégrité que View Manager utilise pour contrôler l'intégrité de ses composants.

Tableau 17-5. Moniteurs d'intégrité

Moniteur	Description
CBMonitor	Contrôle l'intégrité des instances de View Connection Server.
DBMonitor	Contrôle l'intégrité de la base de données des événements.
DomainMonitor	Contrôle l'intégrité du domaine local et de tous les domaines approuvés de l'hôte de View Connection Server.
SGMonitor	Contrôle l'intégrité des services de passerelle de sécurité et des serveurs de sécurité.
TSMonitor	Contrôle l'intégrité des serveurs de transfert.
VCMonitor	Contrôle l'intégrité des serveurs vCenter.

Si un composant contient plusieurs instances, View Manager crée une instance de moniteur séparée pour contrôler chaque instance du composant.

La commande émet toutes les informations sur les moniteurs d'intégrité et les instances de contrôle au format XML.

Options

Tableau 17-6 montre les options que vous pouvez spécifier pour répertorier et afficher des moniteurs d'intégrité.

Tableau 17-6. Options pour répertorier et afficher des moniteurs d'intégrité

Option	Description
`–instanceid` *instance_id*	Spécifie une instance de moniteur d'intégrité.
`–list`	Affiche les moniteurs d'intégrité existants si aucun ID de moniteur d'intégrité n'est spécifié.
`–list –monitorid` *monitor_id*	Affiche les instances de moniteur pour l'ID de moniteur d'intégrité spécifié.
`–monitorid` *monitor_id*	Spécifie un ID de moniteur d'intégrité.

Exemples

Répertoriez tous les moniteurs d'intégrité existants au format XML à l'aide de caractères Unicode.

```
vdmadmin –H –list –xml
```

Répertoriez toutes les instances du moniteur vCenter (VCMonitor) au format XML à l'aide de caractères ASCII.

```
vdmadmin –H –list –monitorid VCMonitor –xml –n
```

Affichez l'intégrité d'une instance de contrôle vCenter spécifiée.

```
vdmadmin –H –monitorid VCMonitor –instanceid 4aec2c99–4879–96b2–de408064d035 –xml
```

Liste et affichage de rapports sur le fonctionnement de View Manager à l'aide de l'option -I

Vous pouvez utiliser la commande `vdmadmin` avec l'option `–I` pour répertorier les rapports disponibles sur le fonctionnement de View Manager et pour afficher les résultats de l'exécution de l'un de ces rapports.

Syntaxe

```
vdmadmin –I [–b authentication_arguments] –list [–xml] [–w | –n]
```

```
vdmadmin –I [–b authentication_arguments] –report report –view view [–startdate yyyy–MM–dd–HH:mm:ss][–enddate yyyy–MM–dd–HH:mm:ss] [–w | –n] –xml | –csv
```

Notes d'utilisation

Vous pouvez utiliser la commande pour afficher les rapports et vues disponibles, et pour afficher les informations que View Manager a enregistré pour un rapport et une vue spécifié.

Vous pouvez également utiliser la commande `vdmadmin` avec l'option `–I` pour générer les messages du journal View dans le format `syslog`. Reportez-vous à la section « Génération de messages de journal des événements View au format Syslog à l'aide de l'option -I », page 474.

Options

Tableau 17-7 montre les options que vous pouvez spécifier pour répertorier et afficher des rapports et des vues.

Tableau 17-7. Options pour répertorier et afficher des rapports et des vues

Option	Description
`–enddate` *yyyy-MM-dd-HH:mm:ss*	Spécifie une limite supérieure pour la date d'informations à afficher.
`–list`	Répertorie les rapports et les vues disponibles.
`–report` *report*	Spécifie un rapport.
`–startdate` *yyyy-MM-dd-HH:mm:ss*	Spécifie une limite inférieure pour la date d'informations à afficher.
`–view` *view*	Spécifie une vue.

Exemples

Répertoriez les rapports et vues disponibles au format XML à l'aide de caractères Unicode.

```
vdmadmin –I –list –xml –w
```

Affichez une liste des événements utilisateur qui se sont produits depuis le 1er août 2010 sous forme de valeurs séparées par des virgules à l'aide de caractères ASCII.

```
vdmadmin –I –report events –view user_events –startdate 2010–08–01–00:00:00 –csv –n
```

Génération de messages de journal des événements View au format Syslog à l'aide de l'option -I

Vous pouvez utiliser la commande `vdmadmin` avec l'option `–I` pour enregistrer des messages d'événement View au format `Syslog` dans des fichiers de journal des événements. De nombreux produits d'analyse tiers requièrent des données `Syslog` de fichier plat comme entrée pour leurs opérations d'analyse.

Syntaxe

```
vdmadmin –I –eventSyslog –disable

vdmadmin –I –eventSyslog –enable –localOnly

vdmadmin –I –eventSyslog –enable –path path

vdmadmin –I –eventSyslog –enable –path path
 –user DomainName\username –password password
```

Notes d'utilisation

Vous pouvez utiliser la commande pour générer des messages de journal des événements View au format `Syslog`. Dans un fichier `Syslog`, les messages de journal des événements View sont mis en forme en paires clé-valeur, ce qui rend les données de journalisation accessibles au logiciel d'analyse.

Vous pouvez également utiliser la commande `vdmadmin` avec l'option `–I` pour répertorier les rapports et les affichages disponibles et pour afficher le contenu d'un rapport spécifié. Reportez-vous à la section « Liste et affichage de rapports sur le fonctionnement de View Manager à l'aide de l'option -I », page 473.

Options

Vous pouvez désactiver ou activer l'option `eventSyslog`. Vous pouvez diriger la sortie `Syslog` vers le système local uniquement ou vers un autre emplacement. La connexion UDP directe vers un serveur `Syslog` est prise en charge avec View 5.2 ou supérieur. Consultez la section « Configurer la journalisation des événements pour des serveurs Syslog » dans le document *Installation de VMware Horizon View*.

Tableau 17-8. Options de génération de messages de journal des événements View au format Syslog

Option	Description
`–disable`	Désactive la journalisation `Syslog`.
`–e|–enable`	Active la journalisation `Syslog`.
`–eventSyslog`	Spécifie que des événements View sont générés au format `Syslog`.
`–localOnly`	Stocke la sortie `Syslog` sur le système local uniquement. Lorsque vous utilisez l'option `–localOnly`, la destination par défaut de la sortie `Syslog` est `%PROGRAMDATA %\VMware\VDM\events\`.
`–password` *password*	Spécifie le mot de passe pour l'utilisateur qui autorise l'accès au chemin de destination spécifié pour la sortie `Syslog`.

Tableau 17-8. Options de génération de messages de journal des événements View au format Syslog (suite)

Option	Description
`–path`	Détermine le chemin d'accès UNC de destination pour la sortie `Syslog`.
`–u|–user` *DomainName\username*	Spécifie le domaine et le nom d'utilisateur qui peuvent accéder au chemin de destination pour la sortie `Syslog`.

Exemples

Désactiver la génération d'événements View au format `Syslog`.

```
vdmadmin –I –eventSyslog –disable
```

Diriger la sortie `Syslog` d'événements View vers le système local uniquement.

```
vdmadmin –I –eventSyslog –enable –localOnly
```

Diriger la sortie `Syslog` d'événements View vers un chemin spécifié.

```
vdmadmin –I –eventSyslog –enable –path path
```

Diriger la sortie `Syslog` d'événements View vers un chemin spécifié qui requiert un accès par un utilisateur de domaine autorisé.

```
vdmadmin –I –eventSyslog –enable –path \\logserver\share\ViewEvents –user mydomain\myuser
 –password mypassword
```

Affectation de postes de travail dédiés à l'aide de l'option -L

Vous pouvez utiliser la commande `vdmadmin` avec l'option `–L` pour affecter des postes de travail d'un pool dédié à des utilisateurs.

Syntaxe

```
vdmadmin –L [–b authentication_arguments] –d desktop –m  machine –u domain\user
```

```
vdmadmin –L [–b authentication_arguments] –d desktop [–m machine | –u domain\user] –r
```

Notes d'utilisation

View Manager affecte des postes de travail à des utilisateurs la première fois qu'ils se connectent à un pool de postes de travail dédié. Dans certaines circonstances, vous voulez peut-être pré-affecter des postes de travail à des utilisateurs. Par exemple, vous voulez peut-être préparer leurs environnements système avant leur connexion initiale. Quand un utilisateur se connecte à un poste de travail que View Manager affecte à un pool dédié, ce poste de travail reste affecté à l'utilisateur pour le reste de la durée de vie de la source de postes de travail. Vous pouvez affecter un utilisateur à une machine virtuelle unique dans un pool dédié.

Vous pouvez affecter un poste de travail à n'importe quel utilisateur autorisé. Vous voulez peut-être faire cela lors de la restauration d'une perte de données View LDAP sur une instance de Serveur de connexion View, ou lorsque vous voulez modifier la propriété d'une source de postes de travail particulière.

Quand un utilisateur se connecte à un poste de travail que View Manager affecte à un pool dédié, ce poste de travail reste affecté à l'utilisateur pour le reste de la durée de vie de la source de postes de travail. Vous voulez peut-être supprimer l'affectation d'un poste de travail d'un utilisateur qui a quitté l'entreprise, qui n'a plus besoin d'accéder au poste de travail ou qui utilisera un poste de travail dans un pool de postes de travail différent. Vous pouvez également supprimer des affectations pour tous les utilisateurs qui accèdent à un pool de postes de travail.

Remarque La commande `vdmadmin -L` n'affecte pas la propriété à des disques persistants de View Composer. Pour affecter des postes de travail de clone lié avec des disques persistants à des utilisateurs, utilisez l'option de menu **[Affecter un utilisateur]** dans View Administrator ou la cmdlet View PowerCLI `Update-UserOwnership`.

Si vous utilisez `vdmadmin -L` pour affecter un poste de travail de clone lié avec un disque persistant à un utilisateur, des résultats inattendus peuvent se produire dans certaines situations. Par exemple, si vous détachez un disque persistant et que vous l'utilisez pour recréer un poste de travail, le poste de travail recréé n'est pas affecté au propriétaire du poste de travail d'origine.

Options

Tableau 17-9 montre les options que vous pouvez spécifier pour affecter un poste de travail à un utilisateur ou pour supprimer une affectation.

Tableau 17-9. Options pour l'affectation de postes de travail dédiés

Option	Description
`-d` *poste de travail*	Spécifie le nom du pool de postes de travail.
`-m` *machine*	Spécifie le nom de la machine virtuelle.
`-r`	Supprime une affectation pour un utilisateur spécifié, ou toutes les affectations d'une machine spécifiée.
`-u` *domain\user*	Spécifie le nom et le domaine d'ouverture de session de l'utilisateur.

Exemples

Affectez la machine machine2 dans le pool de postes de travail dtpool1 à l'utilisateur Jo dans le domaine CORP.

```
vdmadmin -L -d dtpool1 -m machine2 -u CORP\Jo
```

Supprimez les affectations pour l'utilisateur Jo dans le domaine CORP sur des postes de travail dans le pool dtpool1.

```
vdmadmin -L -d dtpool1 -u Corp\Jo -r
```

Supprimez toutes les affectations d'utilisateur sur la machine machine1 dans le pool de postes de travail dtpool3.

```
vdmadmin -L -d dtpool3 -m machine1 -r
```

Affichage d'informations sur les machines à l'aide de l'option -M

Vous pouvez utiliser la commande `vdmadmin` avec l'option `-M` pour afficher des informations sur la configuration de machines virtuelles ou d'ordinateurs physiques.

Syntaxe

```
vdmadmin -M [-b authentication_arguments] [-m machine | [-u domain\user][-d desktop]] [-xml | -csv] [-w | -n]
```

Notes d'utilisation

La commande affiche des informations sur une machine virtuelle ou un ordinateur physique sous-jacent d'un poste de travail.

- Nom d'affichage de la machine.
- Nom du pool de postes de travail.
- État de la machine.

  L'état de la machine peut être l'une des valeurs suivantes : `UNDEFINED`, `PRE_PROVISIONED`, `CLONING`, `CLONINGERROR`, `CUSTOMIZING`, `READY`, `DELETING`, `MAINTENANCE`, `ERROR`, `LOGOUT`.

  La commande n'affiche pas tous les états de machine dynamique, tels que `Connected` ou `Disconnected`, qui sont affichés dans View Administrator.
- SID de l'utilisateur affecté.
- Nom de compte de l'utilisateur affecté.
- Nom de domaine de l'utilisateur affecté.
- État hors ligne d'un poste de travail local (non applicable à la version 4.0 ou antérieure).
- Le chemin d'inventaire de la machine virtuelle (si applicable).
- Date à laquelle la machine a été créée.
- Chemin de modèle de la machine (si applicable).
- URL du serveur vCenter Server (si applicable).

Options

Tableau 17-10 montre les options que vous pouvez utiliser pour spécifier la machine pour laquelle vous voulez afficher des détails.

Tableau 17-10. Options pour l'affichage d'informations sur les machines

Option	Description
`-d` *poste de travail*	Spécifie le nom du pool de postes de travail.
`-m` *machine*	Spécifie le nom de la machine virtuelle.
`-u` *domain\user*	Spécifie le nom et le domaine d'ouverture de session de l'utilisateur.

Exemples

Affichez des informations sur la machine sous-jacente pour le poste de travail dans le pool dtpool2 affecté à l'utilisateur Jo dans le domaine CORP et mettez la sortie au format XML à l'aide de caractères ASCII.

```
vdmadmin -M -u CORP\Jo -d dtpool2 -xml -n
```

Affichez des informations sur la machine machine3 et mettez la sortie au format de valeurs séparées par des virgules.

```
vdmadmin -M -m machine3 -csv
```

Récupération d'espace disque sur des machines virtuelles à l'aide de l'option -M

Vous pouvez utiliser la commande `vdmadmin` avec l'option `–M` pour marquer une machine virtuelle de clone lié pour la récupération d'espace disque. View demande à l'hôte ESXi de récupérer l'espace disque sur le disque du système d'exploitation de clone lié sans attendre que l'espace inutilisé sur le disque du système d'exploitation atteigne le seuil minimal spécifié dans View Administrator.

Syntaxe

```
vdmadmin –M [–b authentication_arguments] –d desktop –m machine –markForSpaceReclamation
```

Notes d'utilisation

Avec cette option, vous pouvez initier la récupération d'espace disque sur une machine virtuelle particulière à des fins de démonstration ou de dépannage.

La récupération d'espace n'a pas lieu si vous exécutez cette commande lorsqu'une période d'interruption est effective.

Les conditions préalables suivantes doivent être respectées pour que vous puissiez récupérer l'espace disque à l'aide de la commande `vdmadmin` avec l'option `–M` :

- Vérifiez que View utilise vCenter Server et ESXi version 5.1 ou supérieure.
- Vérifiez que VMware Tools fourni avec vSphere 5.1 ou supérieur est installé sur la machine virtuelle.
- Vérifiez que la machine virtuelle dispose de la version matérielle virtuelle 9 ou supérieure.
- Dans View Administrator, vérifiez que l'option **[Activer la récupération d'espace]** est sélectionnée pour vCenter Server. Reportez-vous à la section « Autoriser vSphere à récupérer de l'espace disque dans des machines virtuelles de clone lié », page 20.
- Dans View Administrator, vérifiez que l'option **[Récupérer l'espace disque de machine virtuelle]** a été sélectionnée pour le pool de postes de travail. Reportez-vous à la section « Récupérer de l'espace disque sur des postes de travail de clone lié », page 130.
- Vérifiez que la machine virtuelle est activée avant d'initier l'opération de récupération d'espace.
- Vérifiez qu'aucune période d'interruption n'est effective. Reportez-vous à la section « Définir des heures d'interruption pour des opérations ESXi sur des postes de travail View », page 132.

Options

Tableau 17-11. Options de récupération d'espace disque sur des machines virtuelles

Option	Description
`–d` *poste de travail*	Spécifie le nom du pool de postes de travail.
`–m` *machine*	Spécifie le nom de la machine virtuelle.
`–MarkForSpaceReclamation`	Marque la machine virtuelle pour la récupération d'espace disque.

Exemple

Marque la machine virtuelle `machine3` dans le pool de postes de travail `pool1` pour la récupération d'espace disque.

```
vdmadmin –M –d pool1 –m machine3 –markForSpaceReclamation
```

Configuration de filtres de domaine à l'aide de l'option -N

Vous pouvez utiliser la commande vdmadmin avec l'option –N pour contrôler les domaines que View Manager rend disponibles pour les utilisateurs finaux.

Syntaxe

```
vdmadmin –N [–b authentication_arguments] –domains {–exclude | –include | –search} –domain domain
–add [–s connsvr]

vdmadmin –N [–b authentication_arguments] –domains –list [–w | –n] [–xml]

vdmadmin –N [–b authentication_arguments] –domains –list –active [–w | –n] [–xml]

vdmadmin –N [–b authentication_arguments] –domains {–exclude | –include | –search} –domain domain
–remove [–s connsvr]

vdmadmin –N [–b authentication_arguments] –domains {–exclude | –include | –search} –removeall [–s
connsvr]
```

Notes d'utilisation

Spécifiez l'une des options –exclude, –include ou –search pour appliquer une opération à la liste d'exclusion, la liste d'inclusion ou la liste d'exclusion de recherche respectivement.

Si vous ajoutez un domaine à une liste d'exclusion de recherche, le domaine est exclu d'une recherche de domaines automatisée.

Si vous ajoutez un domaine à une liste d'inclusion, le domaine est inclus dans les résultats de la recherche.

Si vous ajoutez un domaine à une liste d'exclusion, le domaine est exclu des résultats de la recherche.

Options

Tableau 17-12 montre les options que vous pouvez spécifier pour configurer des filtres de domaine.

Tableau 17-12. Options pour la configuration de filtres de domaine

Option	Description
–add	Ajoute un domaine à une liste.
–domain *domain*	Spécifie le domaine à filtrer. Vous devez spécifier des domaines par leurs noms NetBIOS et pas par leurs noms DNS.
–domains	Spécifie une opération de filtre de domaine.
–exclude	Spécifie une opération sur une liste d'exclusion.
–include	Spécifie une opération sur une liste d'inclusion.
–list	Affiche les domaines configurés dans la liste d'exclusion de recherche, la liste d'exclusion et la liste d'inclusion sur chaque instance de View Connection Server ou pour le groupe View Connection Server.
–list –active	Affiche les domaines disponibles pour l'instance de View Connection Server sur laquelle vous exécutez la commande.
–remove	Supprime un domaine d'une liste.
–removeall	Supprime tous les domaines d'une liste.

Tableau 17-12. Options pour la configuration de filtres de domaine (suite)

Option	Description
–s *connsvr*	Spécifie que l'opération s'applique aux filtres de domaine sur une instance de View Connection Server. Vous pouvez spécifier l'instance de View Connection Server par son nom ou son adresse IP. Si vous ne spécifiez pas cette option, toutes les modifications que vous faites à la configuration de recherche s'appliquent à toutes les instances de View Connection Server dans le groupe.
–search	Spécifie une opération sur une liste d'exclusion de recherche.

Exemples

Ajoutez le domaine FARDOM à la liste d'exclusion de recherche pour l'instance de View Connection Server csvr1.

```
vdmadmin –N –domains –search –domain FARDOM –add –s csvr1
```

Ajoutez le domaine NEARDOM à la liste d'exclusion pour un groupe View Connection Server.

```
vdmadmin –N –domains –exclude –domain NEARDOM –add
```

Affichez la configuration de recherche de domaine sur les deux instances de View Connection Server dans le groupe, et pour le groupe.

```
C:\ vdmadmin –N –domains –list

Domain Configuration
====================
Cluster Settings
   Include:
   Exclude:
   Search :
     FARDOM
     DEPTX

Broker Settings: CONSVR–1
   Include:
(*)Exclude:
     YOURDOM
   Search :

Broker Settings: CONSVR–2
   Include:
   Exclude:
   Search :
```

View Manager limite la recherche de domaines sur chaque hôte de View Connection Server dans le groupe pour exclure les domaines FARDOM et DEPTX. Les caractères (*) à côté de la liste d'exclusion pour CONSVR-1 indiquent que View Manager exclut le domaine YOURDOM des résultats de la recherche de domaines sur CONSVR-1.

Affichez les filtres de domaine au format XML à l'aide de caractères ASCII.

```
vdmadmin –N –domains –list –xml –n
```

Affichez les domaines disponibles pour View Manager sur l'instance de View Connection Server locale.

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR)
===========================
Primary Domain: MYDOM

Domain            : MYDOM DNS:mydom.mycorp.com
Domain            : YOURDOM DNS:yourdom.mycorp.com
Domain            : FARDOM DNS:fardom.mycorp.com
Domain            : DEPTX DNS:deptx.mycorp.com
Domain            : DEPTY DNS:depty.mycorp.com
Domain            : DEPTZ DNS:deptz.mycorp.com
```

Affichez les domaines disponibles au format XML à l'aide de caractères ASCII.

```
vdmadmin -N -domains -list -active -xml -n
```

Supprimez le domaine NEARDOM de la liste d'exclusion pour un groupe View Connection Server.

```
vdmadmin -N -domains -exclude -domain NEARDOM -remove
```

Supprimez tous les domaines de la liste d'inclusion pour l'instance de View Connection Server csvr1.

```
vdmadmin -N -domains -include -removeall -s csvr1
```

Configuration de filtres de domaine

Vous pouvez configurer des filtres de domaine pour limiter les domaines qu'une instance de View Connection Server ou un serveur de sécurité rend disponibles aux utilisateurs finaux.

View Manager détermine les domaines qui sont accessibles en traversant des relations d'approbation, en commençant par le domaine dans lequel réside une instance de View Connection Server ou un serveur de sécurité. Pour un petit ensemble de domaines bien connectés, View Manager peut déterminer rapidement une liste complète de domaines, mais le temps que prend cette opération augmente car le nombre de domaines accroît ou car la connectivité entre les domaines diminue. View Manager peut également inclure des domaines dans les résultats de recherche que vous ne souhaitez pas proposer aux utilisateurs lorsqu'ils ouvrent une session sur leurs postes de travail.

Si vous avez précédemment défini la valeur de la clé de registre Windows qui contrôle l'énumération de domaines récursifs (`HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\RecursiveDomainEnum`) sur false, la recherche de domaines récursifs est désactivée, et l'instance de View Connection Server n'utilise que le domaine principal. Pour utiliser la fonction de filtrage de domaine, supprimez la clé de registre ou définissez sa valeur sur true et redémarrez le système. Vous devez faire cela pour chaque instance de View Connection Server sur laquelle vous avez défini cette clé.

Tableau 17-13 montre les types de listes de domaines que vous pouvez spécifier pour configurer le filtrage de domaine.

Tableau 17-13. Types de liste de domaines

Type de liste de domaines	Description
Liste d'exclusion de recherche	Spécifie les domaines que View Manager peut traverser lors d'une recherche automatisée. La recherche ignore les domaines inclus dans la liste d'exclusion de recherche, et ne tente pas de rechercher les domaines que le domaine exclu approuve. Vous ne pouvez pas exclure le domaine principal de la recherche.
Liste d'exclusion	Spécifie les domaines que View Manager exclut des résultats d'une recherche de domaines. Vous ne pouvez pas exclure le domaine principal.
Liste d'inclusion	Spécifie les domaines que View Manager n'exclut pas des résultats d'une recherche de domaines. Tous les autres domaines sont supprimés à l'exception du domaine principal.

La recherche de domaines automatisée récupère une liste de domaines, en excluant les domaines que vous spécifiez dans la liste d'exclusion de recherche et les domaines qui sont approuvés par les domaines exclus. View Manager sélectionne la première liste d'exclusion ou d'inclusion non vide dans cet ordre.

1 Liste d'exclusion configurée pour l'instance de View Connection Server.

2 Liste d'exclusion configurée pour le groupe View Connection Server.

3 Liste d'inclusion configurée pour l'instance de View Connection Server.

4 Liste d'inclusion configurée pour le groupe View Connection Server.

View Manager n'applique que la première liste qu'il sélectionne aux résultats de la recherche.

Si vous spécifiez un domaine pour l'inclusion, et que son contrôleur de domaine n'est pas actuellement accessible, View Manager n'inclut pas ce domaine dans la liste de domaines actifs.

Vous ne pouvez pas exclure le domaine principal auquel une instance de View Connection Server ou un serveur de sécurité appartient.

Exemple de filtrage pour inclure des domaines

Vous pouvez utiliser une liste d'inclusion pour spécifier les domaines que View Manager n'exclut pas des résultats d'une recherche de domaine. Tous les autres domaines sont supprimés à l'exception du domaine principal.

Une instance de View Connection Server est associée au domaine MYDOM principal et a une relation d'approbation avec le domaine YOURDOM. Le domaine YOURDOM a une relation d'approbation avec le domaine DEPTX.

Affichez les domaines actuellement actifs de l'instance de View Connection Server.

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR)
===========================
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
Domain: FARDOM DNS: fardom.mycorp.com
Domain: DEPTX DNS:deptx.mycorp.com
Domain: DEPTY DNS:depty.mycorp.com
Domain: DEPTZ DNS:deptz.mycorp.com
```

Les domaines DEPTY et DEPTZ apparaissent dans la liste car ce sont des domaines approuvés du domaine DEPTX.

Spécifiez que l'instance de View Connection Server ne doit rendre disponibles que les domaines YOURDOM et DEPTX, en plus du domaine MYDOM principal.

```
vdmadmin –N –domains –include –domain YOURDOM –add
vdmadmin –N –domains –include –domain DEPTX –add
```

Affichez les domaines actuellement actifs après l'inclusion des domaines YOURDOM et DEPTX.

```
C:\ vdmadmin –N –domains –list –active

Domain Information (CONSVR)
===========================
Primary Domain: MYDOM
Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
Domain: DEPTX DNS:deptx.mycorp.com
```

View Manager applique la liste d'inclusion aux résultats d'une recherche de domaine. Si la hiérarchie de domaine est très complexe ou que la connectivité réseau vers certains domaines est faible, la recherche de domaine peut être lente. Dans de tels cas, utilisez l'exclusion de recherche à la place.

Exemple de filtrage pour exclure des domaines

Vous pouvez utiliser une liste d'exclusion pour spécifier les domaines que View Manager exclut des résultats d'une recherche de domaine.

Un groupe de deux instances de View Connection Server, CONSVR-1 et CONSVR-2, est associé au domaine MYDOM principal et a une relation d'approbation avec le domaine YOURDOM. Le domaine YOURDOM a une relation d'approbation avec les domaines DEPTX et FARDOM.

Le domaine FARDOM se trouve dans un endroit géographique éloigné, et la connectivité réseau vers ce domaine est lente avec une forte latence. Il n'est pas demandé aux utilisateurs dans le domaine FARDOM d'être capable d'accéder au groupe View Connection Server dans le domaine MYDOM.

Affichez les domaines actuellement actifs d'un membre du groupe View Connection Server.

```
C:\ vdmadmin –N –domains –list –active

Domain Information (CONSVR–1)
============================
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
Domain: FARDOM DNS: fardom.mycorp.com
Domain: DEPTX DNS:deptx.mycorp.com
Domain: DEPTY DNS:depty.mycorp.com
Domain: DEPTZ DNS:deptz.mycorp.com
```

Les domaines DEPTY et DEPTZ sont des domaines approuvés du domaine DEPTX.

Pour améliorer les performances de connexion de clients View, excluez le domaine FARDOM des recherches effectuées par le groupe View Connection Server.

```
vdmadmin –N –domains –search –domain FARDOM –add
```

La commande affiche les domaines actuellement actifs après l'exclusion du domaine FARDOM de la recherche.

```
C:\ vdmadmin –N –domains –list –active

Domain Information (CONSVR–1)
============================
```

```
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
Domain: DEPTX DNS:deptx.mycorp.com
Domain: DEPTY DNS:depty.mycorp.com
Domain: DEPTZ DNS:deptz.mycorp.com
```

Étendez la liste d'exclusion de recherche pour exclure le domaine DEPTX et tous ses domaines approuvés de la recherche de domaines pour toutes les instances de View Connection Server dans un groupe. Empêchez également le domaine YOURDOM d'être disponible sur CONSVR-1.

```
vdmadmin –N –domains –search –domain DEPTX –add
vdmadmin –N –domains –exclude –domain YOURDOM –add –s CONSVR–1
```

Affichez la nouvelle configuration de recherche de domaines.

```
C:\ vdmadmin –N –domains –list

Domain Configuration
====================
Cluster Settings
   Include:
   Exclude:
   Search :
     FARDOM
     DEPTX

Broker Settings: CONSVR–1
   Include:
(*)Exclude:
     YOURDOM
   Search :

Broker Settings: CONSVR–2
   Include:
   Exclude:
   Search :
```

View Manager limite la recherche de domaines sur chaque hôte de View Connection Server dans le groupe pour exclure les domaines FARDOM et DEPTX. Les caractères (*) à côté de la liste d'exclusion pour CONSVR-1 indiquent que View Manager exclut le domaine YOURDOM des résultats de la recherche de domaines sur CONSVR-1.

Sur CONSVR-1, affichez les domaines actuellement actifs.

```
C:\ vdmadmin –N –domains –list –active

Domain Information (CONSVR–1)
=============================
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
```

Sur CONSVR-2, affichez les domaines actuellement actifs.

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR-2)
============================
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
```

Affichage des postes de travail et des règles d'utilisateurs non autorisés à l'aide des options -O et -P

Vous pouvez utiliser la commande `vdmadmin` avec les options `-O` et `-P` pour afficher les postes de travail et les règles affectés à des utilisateurs qui ne sont plus autorisés à utiliser le système.

Syntaxe

```
vdmadmin -O [-b authentication_arguments] [-ld | -lu] [-w | -n] [-xml [-noxslt | -xsltpath path]]

vdmadmin -P [-b authentication_arguments] [-ld | -lu] [-w | -n] [-xml [-noxslt | -xsltpath path]]
```

Notes d'utilisation

Si vous révoquez l'autorisation d'un utilisateur sur un poste de travail persistant ou sur un système physique, l'autorisation de poste de travail associée n'est pas automatiquement révoquée. Cela peut être acceptable si vous avez interrompu temporairement le compte d'un utilisateur, ou si l'utilisateur est en vacances. Lorsque vous réactivez l'autorisation, l'utilisateur peut continuer à utiliser le même poste de travail que précédemment. Si un utilisateur a quitté l'entreprise, les autres utilisateurs ne peuvent pas accéder au poste de travail, et il est considéré comme étant orphelin. Vous voulez peut-être aussi examiner des règles qui sont affectées à des utilisateurs non autorisés.

Options

Tableau 17-14 montre les options que vous pouvez spécifier pour afficher les postes de travail et les règles d'utilisateurs non autorisés.

Tableau 17-14. Options pour l'affichage des postes de travail et des règles d'utilisateurs non autorisés

Option	Description
`-ld`	Classe les entrées de sortie par poste de travail.
`-lu`	Classe les entrées de sortie par utilisateur.
`-noxslt`	Spécifie que la feuille de style par défaut ne doit pas être appliquée à la sortie XML.
`-xsltpath` *path*	Spécifie le chemin vers la feuille de style utilisée pour transformer la sortie XML.

Tableau 17-15 montre les feuilles de style que vous pouvez appliquer à la sortie XML pour la transformer en HTML. Les feuilles de style sont situées dans le répertoire `C:\Program Files\VMware\VMware View\server\etc`.

Tableau 17-15. Feuilles de style XSL

Nom du fichier de feuille de style	Description
`list-checkedout-unentitled.xsl`	Transforme des rapports contenant une liste de postes de travail empruntés par des utilisateurs non autorisés.
`unentitled-machines.xsl`	Transforme des rapports contenant une liste de postes de travail non autorisés, groupés par utilisateur ou par système, et qui sont actuellement affectés à un utilisateur. Il s'agit de la feuille de style par défaut.
`unentitled-policies.xsl`	Transforme des rapports contenant une liste de postes de travail avec des règles de niveau utilisateur appliqués à des utilisateurs non autorisés.

Exemples

Affichez les postes de travail affectés à des utilisateurs non autorisés, groupés par poste de travail au format de texte.

```
vdmadmin -O -ld
```

Affichez des postes de travail affectés à des utilisateurs non autorisés, groupés par utilisateur, au format XML à l'aide de caractères ASCII.

```
vdmadmin -O -lu -xml -n
```

Appliquez votre propre feuille de style `C:\tmp\unentitled-users.xsl` et redirigez la sortie vers le fichier `uu-output.html`.

```
vdmadmin -O -lu -xml -xsltpath "C:\tmp\unentitled-users.xsl" > uu-output.html
```

Affichez les règles utilisateur associées à des postes de travail d'utilisateurs non autorisés, groupés par poste de travail, au format XML à l'aide de caractères Unicode.

```
vdmadmin -P -ld -xml -w
```

Appliquez votre propre feuille de style `C:\tmp\unentitled-policies.xsl` et redirigez la sortie vers le fichier `up-output.html`.

```
vdmadmin -P -ld -xml -xsltpath "C:\tmp\unentitled-policies.xsl" > up-output.html
```

Configuration de clients en mode kiosque à l'aide de l'option -Q

Vous pouvez utiliser la commande `vdmadmin` avec l'option `–Q` pour définir des valeurs par défaut et créer des comptes pour des clients en mode kiosque, pour activer l'authentification pour ces clients et pour afficher des informations sur leur configuration.

Syntaxe

`vdmadmin –Q –clientauth –add [–b` *`authentication_arguments`*`] –domain` *`domain_name`*`–clientid` *`client_id`* `[–password "`*`password`*`" | –genpassword] [–ou` *`DN`*`] [–expirepassword | –noexpirepassword] [–group` *`group_name`* `| –nogroup] [–description "`*`description_text`*`"]`

`vdmadmin –Q –disable [–b` *`authentication_arguments`*`] –s` *`connection_server`*

`vdmadmin –Q –enable [–b` *`authentication_arguments`*`] –s` *`connection_server`* `[–requirepassword]`

`vdmadmin –Q –clientauth –getdefaults [–b` *`authentication_arguments`*`] [–xml]`

`vdmadmin –Q –clientauth –list [–b` *`authentication_arguments`*`] [–xml]`

`vdmadmin –Q –clientauth –remove [–b` *`authentication_arguments`*`] –domain` *`domain_name`*`–clientid` *`client_id`*

`vdmadmin –Q –clientauth –removeall [–b` *`authentication_arguments`*`] [–force]`

`vdmadmin –Q –clientauth –setdefaults [–b` *`authentication_arguments`*`] [–ou` *`DN`*`] [ –expirepassword | –noexpirepassword ] [–group` *`group_name`* `| –nogroup]`

`vdmadmin –Q –clientauth –update [–b` *`authentication_arguments`*`] –domain` *`domain_name`*`–clientid` *`client_id`* `[–password "`*`password`*`" | –genpassword] [–description "`*`description_text`*`"]`

Notes d'utilisation

Vous devez exécuter la commande `vdmadmin` sur l'une des instances de Serveur de connexion View dans le groupe qui contient l'instance de Serveur de connexion View que les clients utiliseront pour se connecter à leurs postes de travail.

Lorsque vous configurez des valeurs par défaut pour l'expiration du mot de passe et l'appartenance au groupe Active Directory, ces paramètres sont partagés par toutes les instances de Serveur de connexion View dans un groupe.

Lorsque vous ajoutez un client en mode kiosque, View Manager crée un compte d'utilisateur pour le client dans Active Directory. Si vous spécifiez un nom pour un client, ce nom doit commencer par les caractères « custom- » ou par l'une des autres chaînes de caractères que vous pouvez définir dans ADAM, et il ne peut pas contenir plus de 20 caractères. Vous devez utiliser chaque nom spécifié avec un seul périphérique client.

Vous pouvez définir d'autres préfixes sur « custom- » dans l'attribut à valeurs multiples `pae–ClientAuthPrefix` sous `cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int` dans ADAM sur une instance de Serveur de connexion View. Évitez d'utiliser ces préfixes avec des comptes d'utilisateur ordinaires.

Si vous ne spécifiez pas de nom pour un client, View Manager génère un nom à partir de l'adresse MAC que vous spécifiez pour le périphérique client. Par exemple, si l'adresse MAC est 00:10:db:ee:76:80, le nom de compte correspondant est cm-00_10_db_ee_76_80. Vous ne pouvez utiliser ces comptes qu'avec des instances de Serveur de connexion View que vous activez pour authentifier des clients.

Certains clients légers n'autorisent que les noms de compte qui commencent par les caractères « custom- » ou « cm- » à utiliser avec le mode kiosque.

Un mot de passe généré automatiquement comporte 16 caractères, contient au moins une lettre en majuscule, un lettre en minuscule, un symbole et un nombre, et peut contenir des caractères répétés. Si vous avez besoin d'un mot de passe renforcé, vous devez utiliser l'option `–password` pour spécifier le mot de passe.

Si vous utilisez l'option `-group` pour spécifier un groupe ou si vous avez précédemment défini un groupe par défaut, View Manager ajoute le compte du client à ce groupe. Vous pouvez spécifier l'option `-nogroup` pour empêcher l'ajout du compte à n'importe quel groupe.

Si vous activez une instance de Serveur de connexion View pour authentifier des clients en mode kiosque, vous pouvez facultativement spécifier que les clients doivent fournir un mot de passe. Si vous désactivez l'authentification, les clients ne peuvent pas se connecter à leurs postes de travail.

Même si vous activez ou désactivez l'authentification pour une instance individuelle de Serveur de connexion View, toutes les instances de Serveur de connexion View dans un groupe partagent tous les autres paramètres pour l'authentification client. Vous n'avez qu'à ajouter un client une fois pour toutes les instances de Serveur de connexion View dans un groupe pour pouvoir accepter des demandes du client.

Si vous spécifiez l'option `-requirepassword` lors de l'activation de l'authentification, l'instance de Serveur de connexion View ne peut pas authentifier des clients qui ont généré automatiquement des mots de passe. Si vous modifiez la configuration d'une instance de Serveur de connexion View pour spécifier cette option, de tels clients ne peuvent pas s'authentifier eux-mêmes et ils échouent avec le message d'erreur `Nom d'utilisateur inconnu ou mot de passe incorrect`.

Options

Tableau 17-16 montre les options que vous pouvez spécifier pour configurer des clients en mode kiosque.

Tableau 17-16. Options pour la configuration de clients en mode kiosque

Option	Description
`-add`	Ajoute un compte pour un client en mode kiosque.
`-clientauth`	Spécifie une opération qui configure l'authentification pour un client en mode kiosque.
`-clientid` *client_id*	Spécifie le nom ou l'adresse MAC du client.
`-description` "*description_text*"	Crée une description du compte pour le périphérique client dans Active Directory.
`-disable`	Désactive l'authentification de clients en mode kiosque sur une instance de Serveur de connexion View spécifiée.
`-domain` *domain_name*	Spécifie le domaine pour le compte pour le périphérique client.
`-enable`	Active l'authentification de clients en mode kiosque sur une instance de Serveur de connexion View spécifiée.
`-expirepassword`	Spécifie que le délai d'expiration du mot de passe sur les comptes du client est le même que pour le groupe Serveur de connexion View. Si aucun délai d'expiration n'est défini pour le groupe, les mots de passe n'expirent pas.
`-force`	Désactive l'invite de confirmation lors de la suppression du compte pour un client en mode kiosque.
`-genpassword`	Génère un mot de passe pour le compte du client. Il s'agit du comportement par défaut si vous ne spécifiez pas `-password` ou `-genpassword`.
`-getdefaults`	Obtient les valeurs par défaut qui sont utilisées pour l'ajout de comptes client.
`-group` *group_name*	Spécifie le nom du groupe par défaut auquel les comptes client sont ajoutés. Le nom du groupe doit être spécifié en tant que nom de groupe antérieur à Windows 2000 depuis Active Directory.

Tableau 17-16. Options pour la configuration de clients en mode kiosque (suite)

Option	Description
`–list`	Affiche des informations sur les clients en mode kiosque et sur les instances de Serveur de connexion View sur lesquelles vous avez activé l'authentification de clients en mode kiosque.
`–noexpirepassword`	Spécifie que le mot de passe sur un compte n'expire pas.
`–nogroup`	Lors de l'ajout d'un compte pour un client, spécifie que le compte du client n'est pas ajouté au groupe par défaut. Lors de la définition des valeurs par défaut pour des clients, efface le paramètre du groupe par défaut.
`–ou` *DN*	Spécifie le nom unique de l'unité d'organisation à laquelle les comptes client sont ajoutés. Par exemple : OU=kiosk-ou,DC=myorg,DC=com **Remarque** Vous ne pouvez pas utiliser l'option `–setdefaults` pour modifier la configuration d'une unité d'organisation.
`–password` "*password*"	Spécifie un mot de passe explicite pour le compte du client.
`–remove`	Supprime le compte pour un client en mode kiosque.
`–removeall`	Supprime les comptes de tous les clients en mode kiosque.
`–requirepassword`	Spécifie que des clients en mode kiosque doivent fournir des mots de passe. View Manager n'acceptera pas des mots de passe générés pour les nouvelles connexions.
`–s` *connection_server*	Spécifie le nom NetBIOS de l'instance de Serveur de connexion View sur laquelle activer ou désactiver l'authentification de clients en mode kiosque.
`–setdefaults`	Définit les valeurs par défaut qui sont utilisées pour l'ajout de comptes client.
`–update`	Met à jour un compte pour un client en mode kiosque.

Exemples

Définissez les valeurs par défaut pour l'unité d'organisation, l'expiration du mot de passe et l'appartenance à un groupe de clients.

```
vdmadmin –Q –clientauth –setdefaults –ou "OU=kiosk–ou,DC=myorg,DC=com" –noexpirepassword –group kc–grp
```

Obtenez les valeurs par défaut actuelles de clients au format de texte brut.

```
vdmadmin –Q –clientauth –getdefaults
```

Obtenez les valeurs par défaut actuelles de clients au format XML.

```
vdmadmin –Q –clientauth –getdefaults –xml
```

Ajoutez un compte pour un client spécifié par son adresse MAC au domaine MYORG, et utilisez les paramètres par défaut pour le groupe kc-grp.

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid 00:10:db:ee:76:80 –group kc–grp
```

Ajoutez un compte pour un client spécifié par son adresse MAC au domaine MYORG, et utilisez un mot de passe généré automatiquement.

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid 00:10:db:ee:76:80 –genpassword –ou "OU=kiosk–ou,DC=myorg,DC=com" –group kc–grp
```

Ajoutez un compte pour un client nommé et spécifiez un mot de passe à utiliser avec le client.

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid custom–Terminal21 –password "guest" –ou
"OU=kiosk–ou,DC=myorg,DC=com" –description "Terminal 21"
```

Mettez à jour un compte pour un client, en spécifiant un nouveau mot de passe et du texte descriptif.

```
vdmadmin –Q –clientauth –update –domain MYORG –clientid custom–Terminal21 –password "Secret1!" –
description "Foyer Entry Workstation"
```

Supprimez le compte pour un client kiosque spécifié par son adresse MAC du domaine MYORG.

```
vdmadmin –Q –clientauth –remove –domain MYORG –clientid 00:10:db:ee:54:12
```

Supprimez les comptes de tous les clients sans invite de confirmation de la suppression.

```
vdmadmin –Q –clientauth –removeall –force
```

Activez l'authentification de clients pour l'instance de Serveur de connexion View csvr-2. Les clients avec des mots de passe générés automatiquement peuvent s'authentifier eux-mêmes sans fournir de mot de passe.

```
vdmadmin –Q –enable –s csvr–2
```

Activez l'authentification de clients pour l'instance de Serveur de connexion View csvr-3, et demandez que les clients spécifient leurs mots de passe à View Client. Les clients avec des mots de passe générés automatiquement ne peuvent pas s'authentifier eux-mêmes.

```
vdmadmin –Q –enable –s csvr–3 –requirepassword
```

Désactivez l'authentification de clients pour l'instance de Serveur de connexion View csvr-1.

```
vdmadmin –Q –disable –s csvr–1
```

Affichez des informations sur des clients au format de texte. Le client cm-00_0c_29_0d_a3_e6 possède un mot de passe généré automatiquement, et il ne requiert pas d'utilisateur final ou de script d'application pour spécifier ce mot de passe à View Client. Le client cm-00_22_19_12_6d_cf possède un mot de passe spécifié explicitement et requiert un utilisateur final pour le fournir. L'instance de Serveur de connexion View CONSVR2 accepte les demandes d'authentification depuis des clients avec des mots de passe générés automatiquement. CONSVR1 n'accepte pas les demandes d'authentification depuis des clients en mode kiosque.

```
C:\ vdmadmin –Q –clientauth –list
Client Authentication User List
================================
GUID              : 94be6344–0c9b–4a92–8d54–1brc1c2dc282
ClientID          : cm–00_0c_29_0d_a3_e6
Domain            : myorg.com
Password Generated: true

GUID              : 471d9d35–68b2–40ee–b693–56a7d92b2e25
ClientID          : cm–00_22_19_12_6d_cf
Domain            : myorg.com
Password Generated: false

Client Authentication Connection Servers
========================================
Common Name                   : CONSVR1
Client Authentication Enabled : false
Password Required             : false

Common Name                   : CONSVR2
Client Authentication Enabled : true
Password Required             : false
```

Affichage du premier utilisateur d'un poste de travail à l'aide de l'option -R

Vous pouvez utiliser la commande `vdmadmin` avec l'option `–R` pour en savoir plus sur l'affectation initiale d'un poste de travail géré. Par exemple, en cas de perte de données LDAP, vous pouvez avoir besoin de ces informations pour pouvoir affecter de nouveau des postes de travail à des utilisateurs.

Remarque La commande `vdmadmin` avec l'option `–R` fonctionne uniquement sur les postes de travail antérieurs à View Agent 5.1. Sur les postes de travail exécutant View Agent 5.1 et versions supérieures, cette option ne fonctionne pas. Pour localiser le premier utilisateur d'un poste de travail, utilisez la base de données des événements pour déterminer les utilisateurs connectés au poste de travail.

Syntaxe

```
vdmadmin –R –i network_address
```

Notes d'utilisation

Vous ne pouvez pas utiliser l'option `–b` pour exécuter cette commande en tant qu'utilisateur privilégié. Vous devez avoir ouvert une session en tant qu'utilisateur dans le rôle **Administrateur** .

Options

L'option `–i` spécifie l'adresse IP du poste de travail.

Exemples

Affichez le premier utilisateur qui a accédé à la machine à l'adresse IP 10.20.34.120.

```
vdmadmin –R –i 10.20.34.120
```

Suppression de l'entrée pour une instance de Serveur de connexion View ou un serveur de sécurité à l'aide de l'option -S

Vous pouvez utiliser la commande `vdmadmin` avec l'option `–S` pour supprimer l'entrée d'une instance de Serveur de connexion View ou d'un serveur de sécurité depuis la configuration de View Manager.

Syntaxe

```
vdmadmin –S [–b authentication_arguments] –r –s server
```

Notes d'utilisation

Pour garantir une disponibilité élevée, View Manager vous permet de configurer une ou plusieurs instances de Serveur de connexion View réplicas dans un groupe Serveur de connexion View. Si vous désactivez une instance de Serveur de connexion View dans un groupe, l'entrée du serveur est conservée dans la configuration de View Manager.

Vous pouvez également utiliser la commande `vdmadmin` avec l'option `–S` pour supprimer un serveur de sécurité de votre environnement View. Vous n'avez pas à utiliser cette option si vous prévoyez de mettre à niveau ou de réinstaller un serveur de sécurité sans le supprimer définitivement.

Pour rendre la suppression définitive, effectuez les tâches suivantes :

1 Désinstallez l'instance de Serveur de connexion View ou le serveur de sécurité de l'ordinateur Windows Server en exécutant le programme d'installation de Serveur de connexion View.

2 Supprimez le programme Adam Instance VMwareVDMDS de l'ordinateur Windows Server en exécutant l'outil Ajout/Suppression de programmes.

3 Sur une autre instance de Serveur de connexion View, utilisez la commande `vdmadmin` pour supprimer l'entrée pour l'instance de Serveur de connexion View ou le serveur de sécurité désinstallé(e) depuis la configuration.

Si vous voulez réinstaller View sur les systèmes supprimés sans répliquer la configuration View du groupe d'origine, redémarrez tous les hôtes de Serveur de connexion View dans le groupe d'origine avant d'exécuter la réinstallation. Cela évite aux instances réinstallées de Serveur de connexion View de recevoir des mises à jour de configuration de leur groupe d'origine.

Options

L'option `–s` spécifie le nom NetBIOS de l'instance de Serveur de connexion View ou du serveur de sécurité à supprimer.

Exemples

Supprimez l'entrée de l'instance de Serveur de connexion View connsvr3.

```
vdmadmin –S –r –s connsvr3
```

Définition de la limite de division pour la publication de packages View Transfer Server à l'aide de l'option -T

Vous pouvez utiliser la commande `vdmadmin` avec l'option `–T` pour définir la limite de division pour la publication de packages View Transfer Server. Vous voulez peut-être spécifier une limite de division si vous utilisez un cache proxy qui définit une taille d'objet maximale pour son cache.

Syntaxe

```
vdmadmin –T [–packagelimit  size]
```

Notes d'utilisation

Sur un réseau avec un cache proxy, vous pouvez améliorer les performances en limitant la taille de fichiers de package View Transfer Server publiés pour que leur taille ne soit pas supérieure à la taille d'objet maximale du cache. Si vous spécifiez une limite de division, View Transfer Server divise un fichier de package en parties que ne dépassent pas la limite.

Options

L'option `–packagelimit` spécifie la taille de la limite de division en octets. Si vous ne spécifiez pas cette option, la commande renvoie la limite de division actuelle.

Exemples

Définissez la limite de division sur 100 Mo.

```
vdmadmin –T –packagelimit 104857600
```

Affichez la limite de division actuelle.

```
vdmadmin –T
```

Affichage d'informations sur les utilisateurs à l'aide de l'option -U

Vous pouvez utiliser la commande `vdmadmin` avec l'option `–U` pour afficher des informations détaillées sur les utilisateurs.

Syntaxe

`vdmadmin –U [–b` *`authentication_arguments`*`] –u` *`domain\user`* `[–w | –n] [–xml]`

Notes d'utilisation

La commande affiche des informations sur un utilisateur obtenues après d'Active Directory et de View Manager.

- Des détails d'Active Directory sur le compte de l'utilisateur.
- L'appartenance à des groupes Active Directory.
- Les autorisations de poste de travail, y compris l'ID de poste de travail, le nom d'affichage, une description, le dossier et si un poste de travail a été désactivé.
- affectations ThinApp
- Les rôles d'administrateur, y compris les droits d'administration d'un utilisateur et les dossiers dans lesquels il a ces droits.

Options

L'option `–u` spécifie le nom et le domaine de l'utilisateur.

Exemples

Affichez des informations sur l'utilisateur Jo dans le domaine CORP au format XML à l'aide des caractères ASCII.

```
vdmadmin –U –u CORP\Jo –n –xml
```

Décryptage de la machine virtuelle d'un poste de travail local à l'aide de l'option -V

Présentation sécurise la machine virtuelle d'un poste de travail local en cryptant son image de base. Si vous ne parvenez pas à alimenter ou à restituer le poste de travail local, vous pouvez utiliser la commande `vdmadmin` avec l'option `–V` pour décrypter la machine virtuelle de façon à en restaurer certaines données.

Syntaxe

`vdmadmin –V –rescue [–b` *`authentication_arguments`*`] –d` *`desktop`* `–u` *`domain\user`* `–infile` *`path_to_VM_file`*

Notes d'utilisation

Pour décrypter une machine virtuelle complète, copiez tous ses fichiers depuis la machine client. Spécifiez le nom du fichier de configuration de la machine virtuelle VMware (fichier VMX) comme argument de l'option `–infile`.

Pour décrypter un seul disque d'une machine virtuelle, copiez tous les fichiers de disque virtuel VMware (fichier VMDK) correspondant à ce disque. Si vous avez créé le poste de travail local à partir d'un poste de travail de clone lié, vous devez également copier le sous-dossier contenant les fichiers VMDK de l'image de base. Spécifiez le nom du fichier VMDK du disque comme argument de l'option `–infile`. Ne sélectionnez pas un fichier VMDK correspondant à une partition de disque.

La commande `vdmadmin` écrit les fichiers décryptés dans un sous-dossier nommé `rescued`.

Le décryptage échoue si la clé d'authentification correcte n'est pas disponible dans la configuration View LDAP, ou si l'un des fichiers de la machine virtuelle est corrompu ou manquant.

Options

Tableau 17-17 affiche les options que vous devez définir pour décrypter une machine virtuelle complète ou l'un de ses disques.

Tableau 17-17. Options de décryptage de la machine virtuelle d'un poste de travail local

Option	Description
`–d` *poste de travail*	Spécifie le nom du pool de postes de travail.
`–infile` *path_to_VM_file*	Spécifie le chemin d'accès au fichier VMX ou VMDK pour la machine virtuelle du poste de travail.
`–u` *domain\user*	Spécifie le domaine et le nom de l'utilisateur final du poste de travail local.

Exemples

Décryptez une machine virtuelle complète en sélectionnant son fichier VMX.

```
vdmadmin –V –rescue –d lmdtpool –u MYCORP\jo –infile
"J:\Temp\LMDT_Recovery\CN=lmdtpool,OU=Applications,DC=mycorp,DC=com.vmx"
```

Décryptez la version actuelle du disque `scsi00` de la machine virtuelle en sélectionnant son fichier VMDK.

```
vdmadmin –V –rescue –d lmdtpool –u MYCORP\jo –infile
"J:\Temp\LMDT_Recovery\52e52b7c26a2f683-42b945f934e0fbb2-scsi00-000001.vmdk"
```

Récupération d'un poste de travail en utilisant l'option -V lorsque le poste de travail a été modifié dans le datacenter

Lorsqu'une opération en mode local, telle qu'un emprunt, une restitution ou une réplication, est exécutée, View valide le fait que la machine virtuelle du poste de travail View dans vCenter Server n'a pas été modifiée depuis la dernière synchronisation avec le poste de travail local View. Si un disque de machine virtuelle dans vCenter Server a été modifié et que le disque ne corresponde pas à la version du poste de travail local, vous pouvez utiliser la commande `vdmadmin` avec l'option –V pour conserver les données sur le poste de travail local et la machine virtuelle vCenter Server et faire en sorte que les deux versions soient synchronisées.

Syntaxe

```
vdmadmin –V –recoverClientVM –d desktop_pool –m virtual_machine

vdmadmin –V –recoverServerVM –d desktop_pool –m virtual_machine
```

Notes d'utilisation

Lorsqu'un poste de travail View est emprunté, un snapshot est créé dans vCenter Server afin de préserver l'état de la machine virtuelle. La version vCenter Server du poste de travail est verrouillée pour qu'aucun autre utilisateur ne puisse y accéder.

Si vSphere permet de déverrouiller une machine virtuelle et que la machine virtuelle soit activée par erreur, la machine virtuelle vCenter Server dans le datacenter et celle dans le poste de travail local ne sont plus synchronisées. Par exemple, une machine virtuelle peut être déverrouillée pendant une mise à niveau vCenter Server.

Lorsqu'une opération en mode local est démarrée ou reprise, View utilise l'ID de contenu (CID) du disque de la machine virtuelle pour déterminer si un disque vCenter Server a été modifié depuis la dernière synchronisation entre un disque vCenter Server et le disque correspondant du poste de travail local. Si la machine virtuelle vCenter Server dans le datacenter et celle du poste de travail local ne sont pas identiques, l'opération en mode local est arrêtée et l'utilisateur reçoit le message suivant :

```
This desktop has been modified at the datacenter. Please contact your system administrator (Ce poste de travail a été modifié dans le datacenter. Contactez l'administrateur système.)
```

Vous pouvez récupérer la machine virtuelle du poste de travail local, la machine virtuelle vCenter Server ou les deux versions, en fonction de l'opération en mode local qui était en cours d'exécution.

Récupération de la version de poste de travail local de la machine virtuelle

Si un poste de travail est complètement emprunté ou qu'un utilisateur restitue ou réplique un poste de travail et que la machine virtuelle vCenter Server soit modifiée, l'utilisateur peut disposer de données importantes sur le poste de travail local.

Vous pouvez récupérer la version du poste de travail local en utilisant la commande `vdmadmin` avec l'option `–V –recoverClientVM`. Cette option ramène la machine virtuelle vCenter Server au snapshot créé lors de la dernières synchronisation. Vous pouvez demander à l'utilisateur de redémarrer l'opération de restitution.

Récupération de la version vCenter Server de la machine virtuelle

Si un poste de travail est complètement emprunté ou qu'un utilisateur emprunte un poste de travail et que la machine virtuelle vCenter Server dans le datacenter ait été modifiée, vous avez peut-être installé des applications ou exécuté des mises à jour importantes sur la machine virtuelle vCenter Server.

Vous pouvez récupérer la version vCenter Server en utilisant la commande `vdmadmin` avec l'option `–V –recoverServerVM`. Cette option crée un snapshot de la machine virtuelle vCenter Server, supprime l'ancien snapshot et restaure la machine virtuelle. Au cours d'une restauration, le poste de travail local View est supprimé. Ensuite, vous pouvez demander à l'utilisateur de redémarrer l'opération d'emprunt.

Récupération des deux versions de la machine virtuelle

Dans une situation particulière dans laquelle un poste de travail est complètement emprunté et aucune restitution ou réplication n'était en cours lorsque la machine virtuelle vCenter Server a été ouverte, vous pouvez conserver les machines virtuelles clientes et vCenter Server. Il se peut que du contenu utile valide ait été créé sur les deux machines virtuelles. Dans vCenter Server, vous pouvez cloner la machine virtuelle vCenter Server pour conserver une copie identique. Ensuite, vous pouvez utiliser la commande `vdmadmin` avec l'option `–V –recoverClientVM` pour récupérer la machine virtuelle cliente.

Options

Tableau 17-18. Options de récupération de la version cliente ou vCenter Server d'un poste de travail local

Option	Description
`–recoverClientVM`	Récupère une machine virtuelle de poste de travail local résidant sur un système client. La machine virtuelle vCenter Server est ramenée au snapshot qui a été créé lors de la dernière synchronisation.
`–recoverServerVM`	Récupère une machine virtuelle vCenter Server en créant un snapshot de la machine virtuelle. L'ancien snapshot est supprimé. La machine virtuelle est restaurée, ce qui supprime la machine virtuelle du poste de travail local.
`–d` *desktop_pool*	Spécifie le nom du pool de postes de travail.
`–m` *virtual_machine*	Spécifie le nom de la machine virtuelle du poste de travail local.

Exemples

Récupération d'un machine virtuelle de poste de travail local résidant sur un système client.

```
vdmadmin –V –recoverClientVM –d lmdtpool –m machine1
```

Récupération d'une machine virtuelle vCenter Server et restauration de la machine virtuelle.

```
vdmadmin –V –recoverServerVM –d lmdtpool –m machine2
```

Déverrouillage ou verrouillage de machines virtuelles à l'aide de l'option -V

Vous pouvez utiliser la commande `vdmadmin` avec l'option `–V` pour déverrouiller ou verrouiller des machines virtuelles dans le datacenter.

Syntaxe

```
vdmadmin –V [–b authentication_arguments] –e –d desktop –m machine [–m machine] ...
vdmadmin –V [–b authentication_arguments] –e –vcdn vCenter_dn –vmpath inventory_path
vdmadmin –V [–b authentication_arguments] –p –d desktop –m machine [–m machine] ...
vdmadmin –V [–b authentication_arguments] –p –vcdn vCenter_dn –vmpath inventory_path
```

Notes d'utilisation

Vous devez uniquement utiliser la commande `vdmadmin` pour déverrouiller ou verrouiller une machine virtuelle si vous rencontrez un problème entraînant un état incorrect d'un poste de travail View. N'utilisez pas la commande pour administrer des postes de travail qui fonctionnent normalement. Par exemple, n'utilisez pas `vdmadmin` pour déverrouiller un poste de travail distant emprunté si vous pouvez utiliser View Administrator pour restaurer la session locale.

Si un poste de travail est verrouillé et ne peut pas être restauré, et que l'entrée pour sa machine virtuelle existe dans ADAM, utilisez les options `–d` et `–m` pour spécifier le pool de postes de travail et la machine virtuelle pour le poste de travail que vous voulez déverrouiller. Vous pouvez utiliser la commande `vdmadmin–M` pour découvrir le nom de la machine virtuelle qui est affectée à un utilisateur.

Si un poste de travail est verrouillé et que l'entrée pour sa machine virtuelle n'existe plus dans ADAM, utilisez les options –vmpath et –vcdn pour spécifier le chemin d'inventaire de la machine virtuelle ainsi que le vCenter Server. Vous pouvez utiliser vCenter Client pour trouver le chemin d'inventaire d'une machine virtuelle pour un poste de travail ou une instance de View Transfer Server sous Home/Inventory/VMs and Templates. Vous pouvez utiliser ADAM ADSI Edit pour trouver le nom unique du serveur vCenter Server sous le titre OU=Properties.

Options

Tableau 17-19 montre les options que vous pouvez spécifier pour déverrouiller ou verrouiller des machines virtuelles.

Tableau 17-19. Options pour le déverrouillage ou le verrouillage de machines virtuelles

Option	Description
–d *desktop*	Spécifie le pool de postes de travail.
–e	Déverrouille une machine virtuelle.
–m *machine*	Spécifie le nom de la machine virtuelle.
–p	Verrouille une machine virtuelle.
–vcdn *vCenter_dn*	Spécifie le nom unique du serveur vCenter Server.
–vmpath *inventory_path*	Spécifie le chemin d'inventaire de la machine virtuelle.

Exemples

Déverrouillez les machines virtuelles machine1 et machine2 dans le pool de postes de travail dtpool3.

```
vdmadmin –V –e –d dtpool3 –m machine1 –m machine2
```

Déverrouillez la machine virtuelle d'une instance de View Transfer Server sur un serveur vCenter Server.

```
vdmadmin –V –e –vcdn  "CN=f1060058–
dde2–4940–947b–5d83757b1787,OU=VirtualCenter,OU=Properties,DC=myorg,DC=com" –vmpath
"/DataCenter1/vm/Desktops/LocalMode/LDwin7"
```

Verrouillez la machine virtuelle machine3 dans le pool de postes de travail dtpool3.

```
vdmadmin –V –p –d dtpool3 –m machine3
```

Détection et résolution des collisions d'entrée LDAP à l'aide de l'option -X

Vous pouvez utiliser la commande vdmadmin avec l'option –X pour détecter et résoudre les entrées LDAP en collision sur des instances de View Connection Server répliquées dans un groupe.

Syntaxe

```
vdmadmin –X [–b authentication_arguments] –collisions [–resolve]
```

Notes d'utilisation

Si des entrées LDAP en double sont créées dans deux instances de View Connection Server ou plus, cela peut entraîner des problèmes d'intégrité des données LDAP dans View. Par exemple, cela peut se produire au cours d'une mise à niveau alors que la réplication LDAP est inopérante. Bien que View Manager recherche cette condition d'erreur à intervalles réguliers, vous pouvez exécuter la commande vdmadmin dans l'une des instances de View Connection Server dans le groupe pour détecter et résoudre les collisions d'entrée LDAP manuellement.

Options

Tableau 17-20 montre les options que vous pouvez spécifier pour détecter et résoudre les entrées LDAP en collision.

Tableau 17-20. Options pour la détection et la résolution des collisions d'entrée LDAP

Option	Description
`–collisions`	Spécifie une opération pour détecter les collisions LDAP dans un groupe View Connection Server.
`–resolve`	Résout toutes les collisions LDAP détectées.

Exemples

Détecter des collisions d'entrée LDAP dans un groupe View Connection Server.

```
vdmadmin –X –collisions
```

Détecter et résoudre des collisions d'entrée LDAP.

```
vdmadmin –X –collisions –resolve
```

Configuration de clients en mode kiosque

18

Vous pouvez configurer des clients sans surveillance qui peuvent obtenir un accès à leurs postes de travail depuis VMware Horizon View.

Un client en mode kiosque est un client léger ou un PC verrouillé qui exécute View Client pour se connecter à une instance de Serveur de connexion View et lancer une session à distance. Les utilisateurs finaux n'ont en général pas besoin d'ouvrir une session pour accéder au périphérique client, même si le poste de travail peut requérir qu'ils fournissent des informations d'authentification pour certaines applications. Ces applications peuvent être des stations de travail de saisie de données médicales, des stations d'enregistrement pour compagnies aériennes, des points libre-service client et des points d'informations pour un accès public.

Vous devez vérifier que l'application du poste de travail implémente les mécanismes d'authentification pour des transactions sécurisées, que le réseau physique est sécurisé contre la falsification et la surveillance de trafic et que tous les périphériques connectés au réseau sont approuvés.

Les clients en mode kiosque prennent en charge les fonctions standard pour l'accès distant telles que la redirection automatique de périphériques USB vers la session à distance et l'impression basée sur l'emplacement.

View Manager utilise la fonction Flexible Authentication dans View 4.5 et supérieur pour authentifier un périphérique client en mode kiosque plutôt que l'utilisateur final. Vous pouvez configurer une instance de Serveur de connexion View pour authentifier des clients qui s'identifient avec leur adresse MAC ou avec un nom d'utilisateur qui commence par les caractères « custom- » ou par une autre chaîne de préfixe que vous avez définie dans ADAM. Si vous configurez un client pour qu'il ait un mot de passe généré automatiquement, vous pouvez exécuter View Client sur le périphérique sans spécifier de mot de passe. Si vous configurez un mot de passe explicite, vous devez spécifier ce mot de passe sur View Client. Comme vous exécutez généralement View Client depuis un script, et que le mot de passe apparaît en texte en clair, vous devez prendre des précautions pour rendre le script illisible pour les utilisateurs sans privilèges.

Seules les instances de Serveur de connexion View que vous activez pour authentifier des clients en mode kiosque peuvent accepter des connexions depuis des comptes qui commencent avec les caractères « cm- » suivis d'une adresse MAC, ou qui commencent par les caractères « custom- » ou par une autre chaîne que vous avez définie. View Client dans View 4.5 et supérieur n'autorise pas la saisie manuelle de noms d'utilisateur à ces formats.

Il est recommandé d'utiliser des instances de Serveur de connexion View dédiées pour traiter des clients en mode kiosque, et pour créer des unités d'organisation et des groupes dédiés dans Active Directory pour les comptes de ces clients. Cette pratique partitionne ces systèmes contre les intrusions injustifiées et facilite la configuration et l'administration des clients.

Configurer des clients en mode kiosque

Pour configurer Active Directory et View Manager pour prendre en charge des clients en mode kiosque, vous devez effectuer plusieurs tâches en séquence.

Prérequis

Vérifiez que vous disposez des privilèges requis pour effectuer les tâches de configuration.

- **Domain Admins (Administrateurs de domaine)** ou **Account Operators (Opérateurs de compte)** dans Active Directory pour modifier les comptes d'utilisateurs et de groupes dans un domaine.
- **Administrators (Administrateurs)**, **Inventory Administrators (Administrateurs d'inventaire)** ou un rôle équivalent pour utiliser View Administrator afin d'autoriser des utilisateurs ou des groupes sur des postes de travail.
- **Administrators (Administrateurs)** ou un rôle équivalent pour exécuter la commande `vdmadmin`.

Procédure

1 Préparer Active Directory et View Manager pour des clients en mode kiosque page 501

Vous devez configurer Active Directory pour accepter les comptes que vous créez pour authentifier des périphériques client. Quand vous créez un groupe, vous devez également autoriser ce groupe sur le pool de postes de travail auquel un client accède. Vous pouvez également préparer le pool de postes de travail que les clients utilisent.

2 Définir des valeurs par défaut pour des clients en mode kiosque page 502

Vous pouvez utiliser la commande `vdmadmin` pour définir les valeurs par défaut pour l'unité d'organisation, l'expiration du mot de passe et l'appartenance de groupe dans Active Directory pour des clients en mode kiosque.

3 Afficher les adresses MAC de périphériques client page 503

Si vous souhaitez créer un compte pour un client basé sur son adresse MAC, vous pouvez utiliser View Client pour découvrir l'adresse MAC du périphérique client.

4 Ajout de comptes pour des clients en mode kiosque page 503

Vous pouvez utiliser la commande `vdmadmin` pour ajouter des comptes pour des clients à la configuration d'un groupe Serveur de connexion View. Après avoir ajouté un client, vous pouvez l'utiliser avec une instance de Serveur de connexion View sur laquelle vous avez activé l'authentification de clients. Vous pouvez également mettre à jour la configuration de clients ou supprimer leurs comptes du système.

5 Activer l'authentification de clients en mode kiosque page 505

Vous pouvez utiliser la commande `vdmadmin` pour activer l'authentification de clients qui tentent de se connecter à leurs postes de travail via une instance de View Connection Server.

6 Vérifier la configuration de clients en mode kiosque page 505

Vous pouvez utiliser la commande `vdmadmin` pour afficher des informations sur des clients en mode kiosque et des instances de View Connection Server qui sont configurées pour authentifier de tels clients.

7 Connecter des postes de travail depuis des clients en mode kiosque page 506

Vous pouvez exécuter View Client à partir de la ligne de commande ou utiliser un script pour connecter un client à une session distante.

Préparer Active Directory et View Manager pour des clients en mode kiosque

Vous devez configurer Active Directory pour accepter les comptes que vous créez pour authentifier des périphériques client. Quand vous créez un groupe, vous devez également autoriser ce groupe sur le pool de postes de travail auquel un client accède. Vous pouvez également préparer le pool de postes de travail que les clients utilisent.

Il est recommandé de créer une unité d'organisation et un groupe séparés pour réduire le temps que vous passez à gérer des clients en mode kiosque. Vous pouvez ajouter des comptes individuels pour des clients qui n'appartiennent à aucun groupe, mais cela crée une surcharge administrative importante si vous configurez un petit nombre de clients.

Procédure

1 Dans Active Directory, créez une unité d'organisation et un groupe séparés à utiliser avec des clients en mode kiosque.

Vous devez spécifier un nom antérieur à Windows 2000 pour le groupe. Vous utilisez ce nom pour identifier le groupe dans la commande `vdmadmin`.

2 Créez l'image ou le modèle de la machine virtuelle cliente.

Vous pouvez utiliser une machine virtuelle gérée par vCenter Server en tant que modèle pour un pool automatisé, en tant que parent pour un pool de clone lié ou en tant que source de postes de travail dans un pool manuel. Vous pouvez également installer et configurer des applications sur la machine virtuelle cliente.

3 Configurez la machine virtuelle client pour que les clients ne soient pas verrouillés lorsqu'ils sont laissés sans surveillance.

View supprime le message de pré-ouverture de session pour les clients se connectant en mode kiosque. Si vous avez besoin d'un événement pour déverouiller l'écran et afficher un message, vous pouvez configurer une application appropriée sur la machine virtuelle cliente.

4 Dans View Administrator, créez le pool de postes de travail que les clients utiliseront et autorisez le groupe sur ce pool.

Par exemple, vous pouvez choisir de créer un pool de postes de travail de clone lié d'affectation flottante comme étant le plus approprié pour la configuration requise de votre application client. Vous pouvez également associer une ou plusieurs applications ThinApp au pool de postes de travail.

Important N'autorisez pas un client ou un groupe sur plusieurs pools de postes de travail. Si vous le faites, View Manager affecte un poste de travail de manière aléatoire à partir des pools sur lesquels un client est autorisé, et génère un événement d'avertissement.

---

5 Si vous souhaitez activer l'impression basée sur l'emplacement pour les clients, configurez le paramètre de stratégie de groupe Active Directory `AutoConnect Location-based Printing for VMware View (Impression basée sur l'emplacement de connexion automatique pour VMware View)`, situé dans l'Éditeur d'objets de stratégie de groupe de Microsoft dans le dossier `Software Settings (Paramètres du logiciel)` sous `Computer Configuration (Configuration ordinateur)`.

6 Configurez d'autres règles dont vous avez besoin pour optimiser et sécuriser les postes de travail View des clients.

Par exemple, vous voulez peut-être remplacer les règles qui connectent des périphériques USB locaux au poste de travail lorsqu'il est lancé ou lorsque les périphériques sont branchés. Par défaut, View Client pour Windows active ces règles pour les clients en mode kiosque.

Exemple : Préparation d'Active Directory pour les clients en mode kiosque

L'intranet d'une entreprise a un domaine MYORG, et son unité d'organisation a le nom unique OU=myorg-ou,DC=myorg,DC=com. Dans Active Directory, vous créez l'unité d'organisation kiosk-ou avec le nom unique OU=kiosk-ou,DC=myorg,DC=com et le groupe kc-grp à utiliser avec des clients en mode kiosque.

Suivant

Définissez des valeurs par défaut pour les clients.

Définir des valeurs par défaut pour des clients en mode kiosque

Vous pouvez utiliser la commande `vdmadmin` pour définir les valeurs par défaut pour l'unité d'organisation, l'expiration du mot de passe et l'appartenance de groupe dans Active Directory pour des clients en mode kiosque.

Vous devez exécuter la commande `vdmadmin` sur l'une des instances de View Connection Server dans le groupe qui contient l'instance de View Connection Server que les clients utiliseront pour se connecter à leurs postes de travail.

Lorsque vous configurez des valeurs par défaut pour l'expiration du mot de passe et l'appartenance au groupe Active Directory, ces paramètres sont partagés par toutes les instances de View Connection Server dans un groupe.

Procédure

- Définissez les valeurs par défaut pour des clients.

  `vdmadmin -Q -clientauth -setdefaults [-b` *`authentication_arguments`*`] [-ou` *`DN`*`] [ -expirepassword | -noexpirepassword ] [-group` *`group_name`* `| -nogroup]`

Option	Description
-expirepassword	Spécifie que le délai d'expiration des mots de passe sur les comptes du client est le même que pour le groupe View Connection Server. Si aucun délai d'expiration n'est défini pour le groupe, les mots de passe n'expirent pas.
-group *group_name*	Spécifie le nom du groupe par défaut auquel les comptes client sont ajoutés. Le nom du groupe doit être spécifié en tant que nom de groupe antérieur à Windows 2000 depuis Active Directory.
-noexpirepassword	Spécifie que les mots de passe sur des comptes client n'expirent pas.
-nogroup	Efface le paramètre du groupe par défaut.
-ou *DN*	Spécifie le nom unique de l'unité d'organisation par défaut à laquelle les comptes client sont ajoutés. Par exemple : OU=kiosk-ou,DC=myorg,DC=com **Remarque** Vous ne pouvez pas utiliser la commande pour modifier la configuration d'une unité d'organisation.

La commande met à jour les valeurs par défaut pour les clients dans le groupe View Connection Server.

Exemple : Définition des valeurs par défaut pour des clients en mode kiosque

Définissez les valeurs par défaut pour l'unité d'organisation, l'expiration du mot de passe et l'appartenance à un groupe de clients.

```
vdmadmin -Q -clientauth -setdefaults -ou "OU=kiosk-ou,DC=myorg,DC=com" -noexpirepassword -group kc-grp
```

Suivant

Recherchez les adresses MAC de périphériques client qui utilisent leur adresse MAC pour l'authentification.

Afficher les adresses MAC de périphériques client

Si vous souhaitez créer un compte pour un client basé sur son adresse MAC, vous pouvez utiliser View Client pour découvrir l'adresse MAC du périphérique client.

Prérequis

Ouvrez une session sur la console du client.

Procédure

- Pour afficher l'adresse MAC, saisissez la commande appropriée à votre plate-forme.

Option	Action
Windows	Saisissez **`C:\Program Files\VMware\VMware View\Client\bin\wswc -printEnvironmentInfo`** View Client utilise l'instance de View Connection Server par défaut que vous avez configurée pour lui. Si vous n'avez pas configuré de valeur par défaut, View Client vous invite à fournir la valeur. La commande affiche l'adresse IP, l'adresse MAC et le nom de machine du périphérique client.
Linux	Saisissez **`vmware-view --printEnvironmentInfo -s`** ***`connection_server`*** Vous devez spécifier l'adresse IP ou le FQDN de l'instance de View Connection Server que View Client utilisera pour se connecter au poste de travail. La commande affiche l'adresse IP, l'adresse MAC, le nom de machine, le domaine, le nom et le domaine de l'utilisateur connecté et le fuseau horaire du périphérique.

Suivant

Ajoutez des comptes pour les clients.

Ajout de comptes pour des clients en mode kiosque

Vous pouvez utiliser la commande `vdmadmin` pour ajouter des comptes pour des clients à la configuration d'un groupe Serveur de connexion View. Après avoir ajouté un client, vous pouvez l'utiliser avec une instance de Serveur de connexion View sur laquelle vous avez activé l'authentification de clients. Vous pouvez également mettre à jour la configuration de clients ou supprimer leurs comptes du système.

Vous devez exécuter la commande `vdmadmin` sur l'une des instances de Serveur de connexion View dans le groupe qui contient l'instance de Serveur de connexion View que les clients utiliseront pour se connecter à leurs postes de travail.

Lorsque vous ajoutez un client en mode kiosque, View Manager crée un compte d'utilisateur pour le client dans Active Directory. Si vous spécifiez un nom pour un client, ce nom doit commencer par une chaîne de préfixe reconnue, telle que « custom- », ou par une autre chaîne de préfixe que vous avez définie dans ADAM, et il ne peut pas contenir plus de 20 caractères. Si vous ne spécifiez pas de nom pour un client, View Manager génère un nom à partir de l'adresse MAC que vous spécifiez pour le périphérique client. Par exemple, si l'adresse MAC est 00:10:db:ee:76:80, le nom de compte correspondant est cm-00_10_db_ee_76_80. Vous ne pouvez utiliser ces comptes qu'avec des instances de Serveur de connexion View que vous activez pour authentifier des clients.

IMPORTANT N'utilisez pas un nom spécifié avec plusieurs périphériques client. Les prochaines versions ne prendront peut-être pas en charge cette configuration.

Procédure

- Exécutez la commande vdmadmin à l'aide des options –domain et –clientid pour spécifier le domaine et le nom ou l'adresse MAC du client.

  vdmadmin –Q –clientauth –add [–b *authentication_arguments*] –domain *domain_name* –clientid *client_id* [–password "*password*" | –genpassword] [–ou *DN*] [–expirepassword | –noexpirepassword] [–group *group_name* | –nogroup] [–description "*description_text*"]

Option	Description
–clientid *client_id*	Spécifie le nom ou l'adresse MAC du client.
–description "*description_text*"	Crée une description du compte pour le périphérique client dans Active Directory.
–domain *domain_name*	Spécifie le domaine pour le client.
–expirepassword	Spécifie que le délai d'expiration du mot de passe sur le compte du client est le même que pour le groupe Serveur de connexion View. Si aucun délai d'expiration n'est défini pour le groupe, le mot de passe n'expire pas.
–genpassword	Génère un mot de passe pour le compte du client. Il s'agit du comportement par défaut si vous ne spécifiez pas –password ou –genpassword. Un mot de passe généré comporte 16 caractères, contient au moins une lettre en majuscule, une lettre en minuscule, un symbole et un nombre, et peut contenir des caractères répétés. Si vous avez besoin d'un mot de passe renforcé, utilisez l'option –password pour spécifier le mot de passe.
–group *group_name*	Spécifie le nom du groupe auquel le compte du client est ajouté. Le nom du groupe doit être spécifié en tant que nom de groupe antérieur à Windows 2000 depuis Active Directory. Si vous avez précédemment défini un groupe par défaut, le compte du client est ajouté à ce groupe.
–noexpirepassword	Spécifie que le mot de passe sur le compte du client n'expire pas.
–nogroup	Spécifie que le compte du client n'est pas ajouté au groupe par défaut.
–ou *DN*	Spécifie le nom unique de l'unité d'organisation à laquelle le compte du client est ajouté. Par exemple : OU=kiosk-ou,DC=myorg,DC=com
–password "*password*"	Spécifie un mot de passe explicite pour le compte du client.

La commande crée un compte d'utilisateur dans Active Directory pour le client dans le domaine et le groupe spécifiés (le cas échéant).

Exemple : Ajout de comptes pour des clients

Ajoutez un compte pour un client spécifié par son adresse MAC au domaine MYORG, à l'aide des paramètres par défaut pour le groupe kc-grp.

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid 00:10:db:ee:76:80 –group kc–grp
```

Ajoutez un compte pour un client spécifié par son adresse MAC au domaine MYORG, à l'aide d'un mot de passe généré automatiquement.

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid 00:10:db:ee:76:80 –genpassword
```

Ajoutez un compte pour un client nommé et spécifiez un mot de passe à utiliser avec le client.

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid custom–Terminal21 –password "guest" –ou
"OU=kiosk–ou,DC=myorg,DC=com" –description "Terminal 21"
```

Ajoutez un compte pour un client nommé à l'aide d'un mot de passe généré automatiquement.

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid custom–Kiosk11 –genpassword –ou "OU=kiosk–
ou,DC=myorg,DC=com" –description "Kiosk 11"
```

Suivant

Activez l'authentification des clients.

Activer l'authentification de clients en mode kiosque

Vous pouvez utiliser la commande `vdmadmin` pour activer l'authentification de clients qui tentent de se connecter à leurs postes de travail via une instance de View Connection Server.

Vous devez exécuter la commande `vdmadmin` sur l'une des instances de View Connection Server dans le groupe qui contient l'instance de View Connection Server que les clients utiliseront pour se connecter à leurs postes de travail.

Même si vous activez l'authentification pour une instance individuelle de View Connection Server, toutes les instances de View Connection Server dans un groupe partagent tous les autres paramètres pour l'authentification client. Vous n'avez qu'à ajouter un compte pour un client une fois seulement. Dans un groupe View Connection Server, toutes les instances de View Connection Server activées peuvent authentifier le client.

Procédure

- Activez l'authentification de clients sur une instance de View Connection Server.

  ```
  vdmadmin –Q –enable [–b authentication_arguments] –s connection_server [–requirepassword]
  ```

Option	Description
–requirepassword	Spécifie que vous avez besoin de clients pour fournir des mots de passe. **IMPORTANT** Si vous spécifiez cette option, l'instance de View Connection Server ne peut pas authentifier des clients qui ont généré automatiquement des mots de passe. Si vous modifiez la configuration d'une instance de View Connection Server pour spécifier cette option, de tels clients ne peuvent pas s'authentifier eux-mêmes et ils échouent avec le message d'erreur `Unknown username or bad password`.
–s *connection_server*	Spécifie le nom NetBIOS de l'instance de View Connection Server sur laquelle activer l'authentification de clients.

  La commande active l'instance de View Connection Server spécifiée pour authentifier des clients.

Exemple : Activation de l'authentification de clients en mode kiosque

Activez l'authentification de clients pour l'instance de View Connection Server csvr-2. Les clients avec des mots de passe générés automatiquement peuvent s'authentifier eux-mêmes sans fournir de mot de passe.

```
vdmadmin –Q –enable –s csvr–2
```

Activez l'authentification de clients pour l'instance de View Connection Server csvr-3, et demandez que les clients spécifient leurs mots de passe à View Client. Les clients avec des mots de passe générés automatiquement ne peuvent pas s'authentifier eux-mêmes.

```
vdmadmin –Q –enable –s csvr–3 –requirepassword
```

Suivant

Vérifiez la configuration des instances de View Connection Server et des clients.

Vérifier la configuration de clients en mode kiosque

Vous pouvez utiliser la commande `vdmadmin` pour afficher des informations sur des clients en mode kiosque et des instances de View Connection Server qui sont configurées pour authentifier de tels clients.

Vous devez exécuter la commande `vdmadmin` sur l'une des instances de View Connection Server dans le groupe qui contient l'instance de View Connection Server que les clients utiliseront pour se connecter à leurs postes de travail.

Procédure

- Affichez des informations sur des clients en mode kiosque et sur l'authentification des clients.

  ```
  vdmadmin –Q –clientauth –list [–b authentication_arguments] [–xml]
  ```

  La commande affiche des informations sur des clients en mode kiosque et les instances de View Connection Server sur lesquelles vous avez activé l'authentification client.

Exemple : Affichage d'informations pour les clients en mode kiosque

Affichez des informations sur des clients au format de texte. Le client cm-00_0c_29_0d_a3_e6 possède un mot de passe généré automatiquement, et il ne requiert pas d'utilisateur final ou de script d'application pour spécifier ce mot de passe à View Client. Le client cm-00_22_19_12_6d_cf possède un mot de passe spécifié explicitement et requiert un utilisateur final pour le fournir. L'instance de View Connection Server CONSVR2 accepte les demandes d'authentification depuis des clients avec des mots de passe générés automatiquement. CONSVR1 n'accepte pas les demandes d'authentification depuis des clients en mode kiosque.

```
C:\ vdmadmin –Q –clientauth –list
Client Authentication User List
================================
GUID              : 94be6344–0c9b–4a92–8d54–1brc1c2dc282
ClientID          : cm–00_0c_29_0d_a3_e6
Domain            : myorg.com
Password Generated: true

GUID              : 471d9d35–68b2–40ee–b693–56a7d92b2e25
ClientID          : cm–00_22_19_12_6d_cf
Domain            : myorg.com
Password Generated: false

Client Authentication Connection Servers
========================================
Common Name                   : CONSVR1
Client Authentication Enabled : false
Password Required             : false

Common Name                   : CONSVR2
Client Authentication Enabled : true
Password Required             : false
```

Suivant

Vérifiez que les clients peuvent se connecter à leurs postes de travail.

Connecter des postes de travail depuis des clients en mode kiosque

Vous pouvez exécuter View Client à partir de la ligne de commande ou utiliser un script pour connecter un client à une session distante.

Vous utilisez généralement un script de commande pour exécuter View Client sur un périphérique client déployé.

Pour voir un exemple de script exécutant View Client sur un système Windows, examinez le fichier `C:\Program Files\VMware\VMware View\Client\bin\kiosk_mode.cmd`.

Remarque Sur un client Windows, les périphériques USB sur le client ne sont pas transférés automatiquement s'ils sont utilisés par une autre application ou un autre service lors du démarrage de la session de poste de travail. Pour View Client à partir de View 4.6.x et antérieur, vous devez vérifier que vous avez installé les pilotes sur le client pour tous les périphériques que vous voulez transférer. Sur les clients Windows et Linux, les périphériques d'interface utilisateur et les lecteurs de carte à puce ne sont pas transférés par défaut.

Procédure

- Pour vous connecter à une session distante, saisissez la commande appropriée à votre plate-forme.

Option	Description	
Windows	Saisissez **`C:\Program Files\VMware\VMware View\Client\bin\wswc -unattended [-serverURL` *`connection_server`*`] [-userName` *`user_name`*`] [-password` *`password`*`]`**	
	`-password` *`password`*	Spécifie le mot de passe pour le compte du client. Si vous avez défini un mot de passe pour le compte, vous devez spécifier ce mot de passe.
	`-serverURL` *`connection_server`*	Spécifie l'adresse IP ou le FQDN de l'instance de View Connection Server que View Client utilisera pour se connecter à son poste de travail. Si vous ne spécifiez pas l'adresse IP ou le FQDN de l'instance de View Connection Server que View Client utilisera pour se connecter à son poste de travail, View Client utilise l'instance de View Connection Server par défaut que vous avez configurée pour lui.
	`-userName` *`user_name`*	Spécifie le nom du compte du client. Si vous voulez qu'un client s'authentifie lui-même à l'aide d'un nom de compte qui commence par une chaîne de préfixe reconnue, telle que « custom- », plutôt qu'avec son adresse MAC, vous devez spécifier ce nom.
Linux	Saisissez **`vmware-view --unattended -s` *`connection_server`* `[--once] [-u` *`user_name`*`] [-p` *`password`*`]`**	
	`--once`	Spécifie que vous ne voulez pas que View Client essaie de nouveau de se connecter en cas d'erreur. **Important** Vous devez généralement spécifier cette option et utiliser le code de sortie pour traiter l'erreur. Sinon, il peut vous sembler difficile de tuer le processus `vmware-view` à distance.
	`-p` *`password`*	Spécifie le mot de passe pour le compte du client. Si vous avez défini un mot de passe pour le compte, vous devez spécifier ce mot de passe.
	`-s` *`connection_server`*	Spécifie l'adresse IP ou le FQDN de l'instance de View Connection Server que View Client utilisera pour se connecter à son poste de travail.
	`-u` *`user_name`*	Spécifie le nom du compte du client. Si vous voulez qu'un client s'authentifie lui-même à l'aide d'un nom de compte qui commence par une chaîne de préfixe reconnue, telle que « custom- », plutôt qu'avec son adresse MAC, vous devez spécifier ce nom.

Si View Manager authentifie le client kiosque et qu'un poste de travail View est disponible, la commande démarre la session distante.

Exemple : Exécution de View Client sur des clients en mode kiosque

Exécutez View Client sur un client Windows dont le nom de compte est basé sur son adresse MAC, et qui possède un mot de passe généré automatiquement.

```
C:\Program Files\VMware\VMware View\Client\bin\wswc –unattended –serverURL consvr2.myorg.com
```

Exécutez View Client sur un client Linux à l'aide d'un nom et d'un mot de passe affectés.

```
vmware–view –unattended –s 145.124.24.100 ––once –u custom–Terminal21 –p "Secret1!"
```

Index

C

D

E

F

G

M

N

O

P

Q

R

S

T

U

V

W