Administration de View

VMware Horizon 7 Version 7.1

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

FR-002001-00

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 © 2014–2017 VMware, Inc. Tous droits réservés. Copyright et informations sur les marques.

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 View

Le document *Administration de View* explique comment configurer et administrer VMware Horizon® 7, notamment comment configurer le Serveur de connexion View, créer des administrateurs, configurer l'authentification utilisateur et les stratégies, et gérer des applications VMware ThinApp® dans View Administrator. Ce document explique également comment gérer et dépanner les composants de View.

Public cible

Ces informations sont destinées à toute personne souhaitant configurer et administrer VMware Horizon 7. Les informations sont destinées aux administrateurs Windows ou Linux expérimentés qui connaissent bien le fonctionnement des datacenters et de la technologie des machines virtuelles.

Utilisation de View Administrator 1

View Administrator est l'interface Web avec laquelle vous configurez le Serveur de connexion View et gérez vos applications et postes de travail distants.

Pour consulter une comparaison des opérations que vous pouvez effectuer avec View Administrator, les applets de commande View et `vdmadmin`, reportez-vous au document *Intégration de View*.

Remarque Dans Horizon 7, View Administrator est appelé Horizon Administrator. Ce document fait référence à Horizon Administrator avec le nom View Administrator.

Ce chapitre aborde les rubriques suivantes :

View Administrator et Serveur de connexion View

View Administrator fournit une interface de gestion Web pour View.

Le Serveur de connexion View peut disposer de plusieurs instances qui servent de serveurs réplica ou de serveurs de sécurité. En fonction de votre déploiement de View, vous pouvez obtenir une interface de View Administrator avec chaque instance d'un Serveur de connexion View.

Utilisez les meilleures pratiques suivantes pour utiliser View Administrator avec un Serveur de connexion View :

- Utilisez le nom d'hôte et l'adresse IP du Serveur de connexion View pour vous connecter à View Administrator. Utilisez l'interface de View Administrator pour gérer le Serveur de connexion View et des serveurs de sécurité ou des serveurs réplica associés.
- Dans un environnement d'espace, vérifiez que tous les administrateurs utilisent le nom d'hôte et l'adresse IP du même Serveur de connexion View pour se connecter à View Administrator. N'utilisez pas le nom d'hôte et l'adresse IP de l'équilibrage de charge pour accéder à une page Web de View Administrator.

Remarque Si vous utilisez des dispositifs Access Point plutôt que des serveurs de sécurité, vous devez utiliser l'API REST Access Point pour gérer les dispositifs Access Point. Pour plus d'informations, consultez le document *Déploiement et configuration d'Access Point*.

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 le 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 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.

Si vous ouvrez votre navigateur sur l'hôte de Serveur de connexion View, utilisez **`https://127.0.0.1`** pour vous connecter et non **`https://localhost`**. Cette méthode renforce la sécurité en évitant les attaques DNS potentielles sur la résolution de `localhost`.

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** afin de modifier la liste des utilisateurs et des groupes ayant un rôle d'administrateur 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'avant et vers l'arrière dans les pages de View Administrator	Cliquez sur le bouton **Précédent** de votre navigateur pour accéder à la page de View Administrator précédemment affichée. Cliquez sur le bouton **Suivant** pour revenir à la page actuelle. Si vous cliquez sur le bouton **Précédent** du navigateur pendant que vous utilisez un assistant ou une boîte de dialogue de View Administrator, vous revenez à la page principale de View Administrator. Les informations vous avez entrées dans l'assistant ou la boîte de dialogue sont perdues. Dans les versions de View antérieures à la version View 5.1, vous ne pouviez pas utiliser les boutons **Précédent** et **Suivant** de votre navigateur pour naviguer dans View Administrator. Des boutons **Précédent** et **Suivant** séparés permettaient la navigation dans View Administrator. Ces boutons sont supprimés dans la version View 5.1.
Création de signets pour les pages View Administrator	Vous pouvez créer des signets pour les pages View Administrator dans votre 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 **Ressources > Machines**, vous pouvez cliquer sur **Pool de postes de travail** pour trier les postes de travail en fonction des pools auxquels ils appartiennent. 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 Machines, vous pouvez cliquer sur **Utilisateurs** pour effectuer un tri secondaire en fonction des utilisateurs à qui des 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 sélectionner **Ressources > Machines**, cliquer sur le titre **Magasin de données**, puis appuyer sur Ctrl+clic sur l'en-tête **État**.

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

Fonction de View Administrator	Description
Personnalisation des colonnes du tableau	Vous pouvez personnaliser l'affichage des colonnes du tableau View Administrator en masquant les colonnes sélectionnées et en verrouillant la première colonne. Cette fonctionnalité vous permet de contrôler l'affichage de grands tableaux, tels que **Catalogue > Pools de postes de travail** qui contiennent de nombreuses colonnes. Cliquez avec le bouton droit sur un en-tête de colonne pour afficher le menu contextuel qui vous permet d'effectuer les actions suivantes : ■ Masquer la colonne sélectionnée. ■ Personnaliser des colonnes. Une boîte de dialogue affiche toutes les colonnes du tableau. Vous pouvez sélectionner les colonnes à afficher ou à masquer. ■ Verrouiller la première colonne. Cette option maintient la colonne de gauche affichée pendant que vous faites défiler horizontalement un tableau comportant plusieurs colonnes. Par exemple, sur la page **Catalogue > Pools de postes de travail**, l'ID du poste de travail reste affiché lorsque vous faites défiler horizontalement le tableau pour voir d'autres caractéristiques du poste de travail.
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 **Catalogue > Pools de postes de travail**, cliquez sur la ligne correspondant à un pool individuel pour activer les commandes de ce pool. Double-cliquez sur la cellule **ID** dans la colonne de gauche pour afficher une nouvelle page qui contient 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 de menus contextuels pour des objets View	Vous pouvez cliquer avec le bouton droit sur des objets View dans les tableaux de View Administrator pour afficher des menus contextuels. Un menu contextuel vous donne accès aux commandes qui agissent sur l'objet View sélectionné. Par exemple, dans la page **Catalogue > Pools de postes de travail**, vous pouvez cliquer avec le bouton droit sur un pool de postes de travail pour afficher des commandes telles que **Ajouter**, **Modifier**, **Supprimer**, **Désactiver (ou Activer) l'approvisionnement**, 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 du serveur de connexion View 2

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

Ce chapitre aborde les rubriques suivantes :

Configuration de vCenter Server et View Composer

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

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 les opérations AD de View Composer

Si vous utilisez View Composer, vous devez créer un compte d'utilisateur dans Active Directory qui permet à View Composer d'effectuer certaines opérations dans Active Directory. View Composer requiert que ce compte joigne les machines virtuelles 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 :

   - Lister le contenu
   - Lire toutes les propriétés
   - Écrire toutes les propriétés
   - Autorisations de lecture
   - Réinitialiser le mot de passe
   - Créer des objets ordinateur
   - Supprimer des objets ordinateur

   Remarque Le nombre d'autorisations requises est moins important si vous sélectionnez le paramètre **Autoriser la réutilisation de comptes d'ordinateurs préexistants** pour un pool de postes de travail. Assurez-vous que les autorisations suivantes sont attribuées au compte d'utilisateur :

   - Lister le contenu
   - Lire toutes les propriétés
   - Autorisations de lecture
   - 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 des domaines View Composer dans l'assistant d'ajout d'une instance de vCenter Server et lorsque vous configurez et déployez des pools de postes de travail de clones liés.

Ajouter des instances de vCenter Server à View

Vous devez configurer View afin qu'il se connecte aux instances de vCenter Server dans votre déploiement de View. vCenter Server crée et gère les machines virtuelles que View utilise dans les pools de postes de travail.

Si vous exécutez des instances de vCenter Server dans un groupe Linked Mode, vous devez ajouter séparément chaque instance de vCenter Server à View.

View 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.

- Configurez un utilisateur de vCenter Server autorisé à effectuer dans vCenter Server les opérations nécessaires à la prise en charge de View. Pour utiliser View Composer, vous devez accorder à l'utilisateur des privilèges supplémentaires.

  Pour plus d'informations sur la configuration d'un utilisateur de vCenter Server pour View, reportez-vous au document *Installation de View*.

- Vérifiez qu'un certificat de serveur TLS/SSL est installé sur l'hôte de vCenter Server. Dans un environnement de production, installez un certificat 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 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 racines de confiance > Certificats** dans les magasins de certificats de l'ordinateur local Windows sur les hôtes du 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.

  Reportez-vous à la section « Importer un certificat racine et des certificats intermédiaires dans un magasin de certificats Windows » dans le document *ViewInstallation de* .

- 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.

- Si vous effectuez une mise à niveau vers vSphere 5.5 ou version ultérieure, vérifiez que des autorisations ont été explicitement attribuées au compte d'administrateur du domaine que vous utilisez en tant qu'utilisateur de vCenter Server pour permettre à un utilisateur local de vCenter Server de se connecter à celui-ci.

- Si vous prévoyez d'utiliser View en mode FIPS, vérifiez que vous disposez de vCenter Server 6.0 ou supérieur et d'hôtes ESXi 6.0 ou supérieurs.

  Pour plus d'informations, reportez-vous à « Installer View en mode FIPS » dans le document *Installation de View*.

- Familiarisez-vous avec les paramètres qui déterminent les limites d'opérations maximales pour vCenter Server et View Composer. Reportez-vous aux sections « Limites 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 distants », page 24.

Procédure

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

2 Sous l'onglet **Serveurs vCenter Server**, cliquez sur **Ajouter**.

3 Dans la zone de texte **Adresse du serveur** des paramètres de vCenter Server, entrez le nom de domaine complet de l'instance de vCenter Server.

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

  Remarque Si vous entrez un serveur à l'aide d'un nom DNS ou d'une URL, View n'effectue pas de recherche DNS pour vérifier si un administrateur a précédemment ajouté ce serveur à View 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 25.

Si View 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 de se connecter au service VMware Horizon View Composer. View Composer peut être installé sur son propre hôte séparé ou sur le même hôte que vCenter Server.

Un mappage un-à-un doit être établi entre chaque service VMware Horizon View Composer et chaque instance de vCenter Server. Un service View Composer peut fonctionner avec une seule instance de vCenter Server. Une instance de vCenter Server ne peut être associée qu'à un seul service VMware Horizon View Composer.

Après le déploiement initial de View, vous pouvez migrer le service VMware Horizon View Composer vers un nouvel hôte pour prendre en charge un déploiement de View qui grandit ou qui évolue. 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 une autre machine », page 155.

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 les opérations AD de View Composer », page 15.
- Vérifiez que vous avez configuré View pour se 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 », page 16.
- Vérifiez que ce service VMware Horizon View Composer n'est pas déjà configuré pour se connecter à une autre instance de vCenter Server.

Procédure

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

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

   b Dans 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 celui du port que vous avez spécifié lors de l'installation du service VMware Horizon 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 Server, 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 celui du port que vous avez spécifié lors de l'installation du service VMware Horizon 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 25.

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

- Votre administrateur Active Directory doit créer un utilisateur View Composer pour les opérations AD. Cet utilisateur de domaine doit avoir l'autorisation d'ajouter et de supprimer des machines virtuelles dans le domaine Active Directory qui contient vos clones liés. Pour plus d'informations sur les autorisations requises pour cet utilisateur, reportez-vous à « Créer un compte d'utilisateur pour les opérations AD de View Composer », page 15.
- 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. Dans la page Domaines View Composer, cliquez sur **Ajouter** pour ajouter l'utilisateur de View Composer aux informations du compte des opérations AD.
2. Saisissez le nom de domaine du domaine Active Directory.

   Par exemple : **`domain.com`**
3. Tapez le nom d'utilisateur de domaine, notamment le nom de domaine, de l'utilisateur de View Composer.

   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. De l'espace peut être récupéré lorsque les machines virtuelles sont mises sous tension et que les utilisateurs interagissent avec leurs postes de travail distants.

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 professionnels de l'information qui installent des applications utilisateur sur des postes de travail distants dédiés peuvent perdre leurs applications personnelles si les postes de travail distants 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 provisionnement.

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

Dans un environnement vSphere 5.1 ou version ultérieure, lorsqu'une machine virtuelle parente est la version matérielle virtuelle 9 ou version ultérieure, 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 version ultérieure, et uniquement sur des machines disposant de la version matérielle virtuelle 9 ou version ultérieure.
- 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.

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, notamment tous les hôtes ESXi d'un cluster, sont à la version 5.1 avec le correctif de téléchargement ESXi 5.1 ESXi510-201212001 ou version ultérieure.

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 version ultérieure. Vous devez sélectionner **Activer la récupération d'espace** si vous effectuez une mise à niveau vers View 5.2 ou version ultérieure depuis View 5.1 ou 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 Horizon 7 lors des tempêtes d'E/S, qui peuvent se produire lorsque de nombreuses machines virtuelles 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 Horizon 7.

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

Vérifiez que View Storage Accelerator est également configuré pour des pools de postes de travail individuels. Pour fonctionner sur un pool de postes de travail, View Storage Accelerator doit être activé pour vCenter Server et pour le pool de postes de travail individuel.

View Storage Accelerator est activé pour un pool de postes de travail par défaut. Vous pouvez activer ou désactiver cette fonctionnalité lors de la création ou de la modification d'un pool. La meilleure approche consiste à activer cette fonctionnalité lorsque vous créez un pool de postes de travail pour la première fois. Si vous activez cette fonctionnalité en modifiant un pool existant, vous devez vous assurer qu'un nouveau réplica et ses disques digest soient créés avant que des clones liés soient provisionnés. Vous pouvez créer un nouveau réplica en recomposant le pool sur un nouveau snapshot ou en rééquilibrant le pool sur une nouvelle banque de données. Les fichiers digest peuvent être configurés uniquement pour des machines virtuelles dans un pool de postes de travail où elles sont désactivées.

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

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 Horizon 7, dans lesquelles des réplicas sont stockés dans une banque de données distincte des clones liés. Bien que les avantages de performance liés à l'utilisation de View Storage Accelerator avec la hiérarchisation de réplica Horizon 7 ne soient pas matériellement importants, certains avantages liés à la capacité peuvent être obtenus en stockant les réplicas sur une banque de données distincte. Par conséquent, cette combinaison est testée et prise en charge.

Important Si vous prévoyez d'utiliser cette fonctionnalité et que vous utilisez plusieurs espaces View qui partagent des hôtes ESXi, vous devez activer la fonction View Storage Accelerator pour tous les pools qui se trouvent sur les hôtes ESXi partagés. Si les paramètres ne sont pas les mêmes sur tous les espaces, cela peut entraîner l'instabilité des machines virtuelles des hôtes ESXi partagés.

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 a reçu le privilège **Hôte > Configuration > Paramètres avancés** dans vCenter Server.

  Consultez les rubriques du document *Installation de View* qui décrivent les privilèges d'Horizon 7 et de View Composer requis pour l'utilisateur de vCenter Server.

Procédure

1. Dans Horizon Administrator, fournissez les renseignements dans 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 du 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 Horizon 7.

Suivant

Configurez des paramètres pour les sessions et les connexions client. Reportez-vous à la section « Configuration de paramètres pour des sessions client », page 28.

Pour régler les paramètres de View Storage Accelerator dans Horizon 7, 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 » dans le document *Configuration des postes de travail virtuels dans Horizon 7*.

Limites d'opérations simultanées pour vCenter Server et View Composer

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

Vous configurez ces options dans le volet Paramètres avancés de la page d'informations sur vCenter Server.

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

Paramètre	Description
Opérations d'approvisionnement de vCenter simultanées max.	Détermine le nombre maximal de demandes simultanées que Serveur de connexion View peut créer pour approvisionner et supprimer des machines virtuelles complètes dans cette instance de vCenter Server. La valeur par défaut est 20. Ce paramètre s'applique uniquement à des machines virtuelles complètes.
Opérations d'alimentation simultanées max.	Détermine le nombre maximal d'opérations d'alimentation (démarrage, arrêt, interruption, etc.) pouvant se dérouler simultanément sur des machines virtuelles gérées par Serveur de connexion View dans cette instance de vCenter Server. La valeur par défaut est 50. Pour obtenir des recommandations sur le calcul d'une valeur pour ce paramètre, consultez « Définition d'un taux d'opérations d'alimentation simultanées pour prendre en charge les tempêtes d'ouverture de session des postes de travail distants », page 24. Ce paramètre s'applique à des machines virtuelles complètes et à des clones liés.
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 des clones liés gérés par cette instance de View Composer. La valeur par défaut est 12. Les sessions actives des postes de travail distants doivent être fermées avant que l'opération de maintenance puisse commencer. Si vous forcez les utilisateurs à fermer leur session dès que l'opération de maintenance commence, le nombre maximal d'opérations simultanées sur les postes de travail distants nécessitant une fermeture de session correspond à la moitié de la valeur configurée. Par exemple, si vous définissez ce paramètre sur 24 et forcez les utilisateurs à fermer leur session, le nombre maximal d'opérations simultanées sur les postes de travail distants nécessitant une fermeture de session est de 12. Ce paramètre ne s'applique qu'aux clones liés.
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 des clones liés gérés par cette instance de View Composer. La valeur par défaut est 8. Ce 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 distants

Le paramètre **Opérations d'alimentation simultanées max** régit le nombre maximal d'opérations d'alimentation simultanées qui peuvent se produire sur des machines virtuelles de poste de travail distant dans une instance de vCenter Server. Cette limite est fixée à 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, reportez-vous à la section « Recommandations sur la planification et les éléments de conception d'architecture » dans le document *Planification de l'architecture de 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.

Le système 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 de View Composer à View, vous devez vérifier que les certificats SSL utilisés pour les instances de vCenter Server et de View Composer sont valides et approuvés par le Serveur de connexion View. Si les certificats par défaut installés avec vCenter Server et View Composer sont toujours en place, vous devez déterminer s'il convient ou non d'accepter les empreintes de ces certificats.

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

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

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

Remarque Vous devez également accepter une empreinte de certificat lorsque vous mettez à niveau une version antérieure et lorsqu'un certificat de vCenter Server ou de 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 de 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 qu'utilisera une instance du Serveur de connexion View. Si le certificat de serveur SAML n'est pas approuvé par le Serveur de connexion View, vous devez déterminer s'il convient ou non d'accepter l'empreinte de certificat. Si vous n'acceptez pas l'empreinte, vous ne pouvez pas configurer l'authentificateur SAML dans View. Une fois l'authentificateur SAML configuré, vous pouvez le reconfigurer dans la boîte de dialogue Modifier le 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 Vérifiez l'empreinte de certificat qui a été configurée pour l'instance de vCenter Server ou de View Composer.

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

   b Accédez au certificat de vCenter Server ou de View Composer.

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

   De la même façon, vérifiez l'empreinte de certificat d'un authentificateur SAML. Le cas échéant, exécutez les étapes précédentes sur l'hôte de l'authentificateur SAML.

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

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

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 de View une instance de vCenter Server

Vous pouvez supprimer la connexion entre View et une instance de vCenter Server. Lorsque vous le faites, View ne gère plus les machines virtuelles créées dans cette instance de vCenter Server.

Prérequis

Supprimez toutes les machines virtuelles associées à l'instance de vCenter Server. Reportez-vous à la section « Supprimer un pool de postes de travail », page 204.

Procédure

1 Cliquez sur **Configuration de View > Serveurs**.

2 Dans l'onglet **vCenter Servers**, sélectionnez l'instance de vCenter Server.

3 Cliquez sur **Supprimer**.

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

4 Cliquez sur **OK**.

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

Supprimer View Composer de View

Vous pouvez supprimer la connexion entre View et le service VMware Horizon View Composer qui est associé à une instance de vCenter Server.

Avant de désactiver la connexion à View Composer, vous devez supprimer de View toutes les machines virtuelles de clone lié créées par View Composer. View vous empêche de supprimer View Composer si des clones liés associés existent toujours. Une fois que la connexion à View Composer est désactivée, View ne peut plus provisionner ni gérer de nouveaux clones liés.

Procédure

1 Supprimez les pools de postes de travail de clone lié qui ont été créés par View Composer.

   a Dans View Administrator, sélectionnez **Catalogue > Pools de postes de travail**.

   b Sélectionnez un pool de postes de travail de clone lié et cliquez sur **Supprimer**.

   Une boîte de dialogue vous avertit que vous allez supprimer de façon permanente de View le pool de postes de travail de clone lié. Si les machines virtuelles de clone lié sont configurées avec des disques persistants, vous pouvez détacher 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 postes de travail de clone lié créé par View Composer.

2 Sélectionnez **Configuration de View > Serveurs**.

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

4 Cliquez sur **Modifier**.

5 Sous Paramètres de View Composer Server, cliquez sur **Modifier**, sélectionnez **Ne pas utiliser View Composer**, puis cliquez sur **OK**.

Vous ne pouvez plus créer de pools 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 avez l'intention d'installer View Composer sur un autre hôte et de reconfigurer View pour se connecter au nouveau service VMware Horizon View Composer, vous devez effectuer des étapes supplémentaires. Reportez-vous à la section « Migrer View Composer sans machines virtuelles de clone lié », page 158.

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 tentez d'ajouter une instance de vCenter Server à View, mais l'ID unique de la nouvelle instance de vCenter Server est en conflit avec celle d'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 > Paramètres de vCenter Server > 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 du Serveur de connexion View

Après avoir terminé la configuration initiale du Serveur de connexion View, vous devez planifier des sauvegardes régulières de vos données de configuration de View et de View Composer.

Pour plus d'informations sur la sauvegarde et la restauration de votre configuration de View, reportez-vous à « Sauvegarde et restauration de données de configuration de View », page 141.

Configuration de paramètres pour des sessions client

Vous pouvez configurer des paramètres généraux qui affectent les sessions et connexions client gérées par une instance du Serveur de connexion View ou un groupe répliqué. Vous pouvez définir la durée du délai d'expiration de la session, afficher des messages de pré-ouverture de session ou d'avertissement, et définir les options de connexion client liées 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 du Serveur de connexion View. Ils affectent toutes les sessions client gérées par une instance du Serveur de connexion View autonome ou un groupe d'instances répliquées.

Vous pouvez également configurer des instances du Serveur de connexion View pour qu'elles utilisent des connexions directes hors tunnel entre des clients Horizon et des postes de travail distants. Pour plus d'informations sur la configuration de connexions directes, reportez-vous à « Configurer le tunnel sécurisé et PCoIP Secure Gateway », page 38.

Prérequis

Familiarisez-vous avec les paramètres généraux. Reportez-vous aux sections « Paramètres généraux pour des sessions client », page 29 et « Paramètres généraux de sécurité des sessions et connexions client », page 33.

Procédure

1 Dans View Administrator, sélectionnez **Configuration de View > Paramètres généraux**.

2 Choisissez s'il convient de configurer des paramètres généraux ou des paramètres de sécurité.

Option	Description
Paramètres généraux globaux	Dans le volet Général, cliquez sur **Modifier**.
Paramètres de sécurité globaux	Dans le volet Sécurité, cliquez sur **Modifier**.

3 Configurez les paramètres généraux.

4 Cliquez sur **OK**.

Suivant

Vous pouvez modifier le mot de passe de récupération de données qui a été fourni lors de l'installation. Reportez-vous à la section « Modifier le mot de passe de récupération de données », page 29.

Modifier le mot de passe de récupération de données

Vous fournissez un mot de passe de récupération de données lorsque vous installez le Serveur de connexion View version 5.1 ou version ultérieure. Après l'installation, vous pouvez modifier ce mot de passe dans View Administrator. Le mot de passe est requis lorsque vous restaurez la configuration de View LDAP à partir d'une sauvegarde.

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

Le mot de passe doit contenir entre 1 et 128 caractères. Suivez les meilleures pratiques de votre entreprise concernant la génération de mots de passe sécurisés.

Procédure

1 Dans View Administrator, sélectionnez **Configuration de View > Paramètres généraux**.

2 Dans le volet Sécurité, cliquez sur **Modifier le mot de passe de récupération de données**.

3 Tapez et retapez le nouveau mot de passe.

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

Remarque Vous pouvez également modifier le mot de passe de récupération de données lorsque vous planifiez la sauvegarde de vos données de configuration View. Reportez-vous à la section « Planifier des sauvegardes de configuration de View », page 142.

Suivant

Lorsque vous employez l'utilitaire `vdmimport` pour restaurer une configuration View de sauvegarde, 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, si des messages de pré-ouverture de session et d'avertissement sont affichés, si View Administrator traite Windows Server comme un système d'exploitation pris en charge pour les postes de travail distants, ainsi que d'autres paramètres.

Les modifications apportées à tout paramètre du tableau suivant prennent effet immédiatement. Vous n'avez pas à redémarrer Serveur de connexion View ou Horizon Client.

Tableau 2-2. Paramètres généraux pour des sessions client

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).
Forcer la déconnexion des utilisateurs	Déconnecte tous les postes de travail et toutes les applications après que le nombre de minutes spécifié s'est écoulé depuis que l'utilisateur s'est connecté à View. Tous les postes de travail et toutes les applications seront déconnectés en même temps, quel que soit le moment auquel l'utilisateur les a ouverts. Pour les clients qui ne prennent pas en charge l'accès distant aux applications, une valeur de délai d'expiration maximale de 1 200 minutes s'applique si la valeur de ce paramètre est **Jamais** ou supérieure à 1 200 minutes. La valeur par défaut est **Après 600 minutes**.
Single sign-on (SSO)	Si SSO est activé, View met en cache les informations d'identification de l'utilisateur afin que ce dernier puisse lancer des applications ou des postes de travail distants sans avoir à ouvrir la session Windows distante. L'option par défaut est **Activé**. Si vous prévoyez d'utiliser la fonctionnalité d'authentification unique réelle, introduite dans Horizon 7 ou version ultérieure, l'authentification unique doit être activée. Avec l'authentification unique réelle, si un utilisateur se connecte avec une méthode n'utilisant pas d'informations d'identification Active Directory, la fonctionnalité d'authentification unique réelle génère des certificats de courte durée, plutôt que des informations d'identification en cache, une fois que les utilisateurs sont connectés à VMware Identity Manager. **Remarque** Si un poste de travail est lancé à partir d'Horizon Client, si le poste de travail est verrouillé, soit par l'utilisateur, soit par Windows conformément à une stratégie de sécurité, et si le poste de travail exécute View Agent 6.0 ou version ultérieure ou Horizon Agent 7.0 ou version ultérieure, le Serveur de connexion View ignore les informations d'identification d'authentification unique de l'utilisateur. L'utilisateur doit fournir des informations d'identification de connexion pour lancer un nouveau poste de travail ou une nouvelle application, ou se reconnecter à une application ou un poste de travail déconnecté. Pour réactiver SSO, l'utilisateur doit se déconnecter du Serveur de connexion View ou quitter Horizon Client, et se reconnecter au Serveur de connexion View. Cependant, si le poste de travail est lancé à partir de Workspace Portal ou VMware Identity Manager et s'il est verrouillé, les informations d'identification d'authentification unique ne sont pas supprimées.

Tableau 2-2. Paramètres généraux pour des sessions client (suite)

Paramètre	Description
Pour les clients prenant en charge les applications. **Si l'utilisateur cesse d'utiliser le clavier et la souris, déconnecter ses applications et supprimer les informations d'identification SSO :**	Protège les sessions d'application en l'absence d'activité de clavier ou de souris sur le périphérique client. Si ce paramètre est défini sur **Après ... minutes**, View, View déconnecte toutes les applications et ignore les informations d'identification SSO au terme du nombre spécifié de minutes sans activité de l'utilisateur. Les sessions de poste de travail ne sont pas déconnectées. L'utilisateur doit ouvrir une nouvelle session pour se reconnecter aux applications déconnectées ou lancer un nouveau poste de travail ou une nouvelle application. Ce paramètre s'applique également à la fonctionnalité d'authentification unique réelle. Une fois les informations d'identification d'authentification unique supprimées, les utilisateurs sont invités à fournir leurs informations d'identification Active Directory. Si des utilisateurs sont connectés à VMware Identity Manager sans utiliser d'informations d'identification AD et qu'ils ne savent pas quelles informations d'identification AD entrer, ils peuvent se déconnecter et se reconnecter à VMware Identity Manager pour accéder à leurs applications et postes de travail distants. **Important** Les utilisateurs doivent savoir que lorsque des applications et des postes de travail sont ouverts, et que des applications sont déconnectées en raison du dépassement de ce délai d'expiration, leur poste de travail reste ouvert. Les utilisateurs ne doivent pas se fier à ce délai d'expiration pour protéger leur poste de travail. Si ce paramètre est défini sur **Jamais**, View ne déconnecte jamais les applications et n'ignore jamais les informations d'identification SSO suite à l'inactivité de l'utilisateur. La valeur par défaut est **Jamais**.
Autres clients. **Supprimer les informations d'identification SSO :**	Supprimer les informations d'identification SSO après le nombre de minutes spécifié. Ce paramètres concerne les clients qui ne prennent pas en charge l'accès à distance aux applications. Si ce paramètre est défini sur **Après ... minutes**, l'utilisateur doit ouvrir une nouvelle session pour se connecter à un poste de travail une fois que le nombre spécifié de minutes s'est écoulé depuis qu'il s'est connecté à View, quelle que soit son activité sur le périphérique client. Si cette option est définie sur **Jamais**, View enregistre les informations d'identification SSO jusqu'à ce que l'utilisateur ferme Horizon Client ou que le délai d'expiration **Forcer la déconnexion des utilisateurs** soit atteint, selon la première de ces éventualités. La valeur par défaut est **Après 15 minutes**.
Activer les mises à jour d'état automatiques	Détermine si les mises à jour s'affichent dans le volet d'état général dans le coin supérieur gauche de View Administrator après quelques minutes. La page Tableau de bord de View Administrator est également mise à jour après quelques minutes. Par défaut, ce paramètre n'est pas activé.
Afficher un message de pré-ouverture de session	Affiche une clause d'exclusion de responsabilité ou un autre message aux utilisateurs d'Horizon Client lorsqu'ils ouvrent une session. Entrez vos informations ou instructions dans la zone de texte de la boîte de dialogue Paramètres généraux. Pour n'afficher aucun message, ne cochez pas la case.

Tableau 2-2. Paramètres généraux pour des sessions client (suite)

Paramètre	Description
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 5 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. Enregistrez le travail non sauvegardé maintenant.`
Activer les postes de travail Windows Server	Détermine si vous pouvez sélectionner des machines Windows Server 2008 R2 et Windows Server 2012 R2 disponibles pour les utiliser comme postes de travail. Lorsque ce paramètre est activé, View Administrator affiche toutes les machines Windows Server disponibles, y compris celles sur lesquelles des composants de serveur View sont installés. **Remarque** Le logiciel Horizon Agent ne peut pas coexister sur la même machine virtuelle ou physique avec tout autre composant logiciel du serveur View, notamment un serveur de sécurité, un Serveur de connexion View ou View Composer.
Effacer les informations d'identification lors de la fermeture d'un onglet pour HTML Access	Supprime les informations d'identification d'un utilisateur du cache lorsque l'utilisateur ferme un onglet qui le connecte à une application ou un poste de travail distant, ou lorsqu'il ferme un onglet qui le connecte à la page de sélection des postes de travail et applications, dans le client HTML Access. Lorsque ce paramètre est activé, View supprime également les informations d'identification du cache dans les scénarios suivants du client HTML Access : ■ Un utilisateur actualise la page de sélection des postes de travail et applications ou la page de session distante. ■ Le serveur présente un certificat auto-signé, un utilisateur lance une application ou un poste de travail distant et l'utilisateur accepte le certificat lorsque l'avertissement de sécurité s'affiche. ■ Un utilisateur exécute une commande URI dans l'onglet qui contient la session distante. Lorsque ce paramètre est désactivé, les informations d'identification restent dans le cache. Cette fonctionnalité est désactivée par défaut. **Remarque** Cette fonctionnalité est disponible dans Horizon 7 version 7.0.2 et ultérieures.
Configuration du serveur Mirage	Vous permet de spécifier l'URL d'un serveur Mirage au format **`mirage://server-name:port`** ou **`mirages://server-name:port`**. Ici, *server-name* correspond au nom du domaine complet. Si vous ne spécifiez pas de numéro de port, le port par défaut 8000 est employé. **Remarque** Vous pouvez remplacer ce paramètre général en spécifiant un serveur Mirage dans les paramètres du pool de postes de travail. La spécification du serveur Mirage dans View Administrator est une alternative à la spécification du serveur Mirage lors de l'installation du client Mirage. Pour déterminer quelles versions de Mirage prennent en charge la spécification de serveur dans View Administrator, consultez la documentation de Mirage, à l'adresse https://www.vmware.com/support/pubs/mirage_pubs.html.

Tableau 2-2. Paramètres généraux pour des sessions client (suite)

Paramètre	Description
Masquer les informations de serveur dans l'interface utilisateur client	Activez ce paramètre de sécurité pour masquer les informations d'URL de serveur dans Horizon Client 4.4 ou version ultérieure.
Masquer la liste de domaines dans l'interface utilisateur client	Activez ce paramètre de sécurité pour masquer le menu déroulant Domaine dans Horizon Client 4.4 ou version ultérieure. Lorsque des utilisateurs se connectent à une instance du Serveur de connexion pour laquelle le paramètre global **Masquer la liste de domaines dans l'interface utilisateur client** est activé, le menu déroulant Domaine est masqué dans Horizon Client et les utilisateurs fournissent des informations sur le domaine dans la zone de texte **Nom d'utilisateur** d'Horizon Client. Par exemple, les utilisateurs doivent entrer leur nom d'utilisateur au format `domain\username` ou `username@domain`. **Important** Si vous activez les paramètres **Masquer les informations de serveur dans l'interface utilisateur client** et **Masquer la liste de domaines dans l'interface utilisateur client** et sélectionnez l'authentification à deux facteurs (RSA SecureID ou RADIUS) pour l'instance du Serveur de connexion, n'appliquez pas la correspondance des noms d'utilisateur Windows. L'application de la correspondance des noms d'utilisateur Windows empêchera les utilisateurs d'entrer des informations sur le domaine dans la zone de texte Nom d'utilisateur et la connexion échouera toujours. Pour plus d'informations, consultez les rubriques concernant l'authentification à deux facteurs dans le document *Administration de View*.

Paramètres généraux de sécurité des sessions et connexions client

Les paramètres de sécurité généraux déterminent si les clients sont réauthentifiés après des interruptions, si le mode de sécurité des messages est activé et si IPSec est employé pour les connexions du serveur de sécurité.

SSL est requis pour toutes les connexions d'Horizon Client et de View Administrator à View. Si votre déploiement de View utilise des équilibrages de charge ou d'autres serveurs intermédiaires clients, vous pouvez décharger SSL sur eux, configurer des connexions non-SSL sur des instances du Serveur de connexion View et des serveurs de sécurité individuels. Reportez-vous à la section « Décharger des connexions SSL sur des serveurs intermédiaires », page 41.

Tableau 2-3. Paramètres généraux de sécurité des sessions et connexions client

Paramètre	Description
Authentifier à nouveau les connexions par tunnel sécurisé après une interruption de réseau	Détermine si les informations d'identification d'utilisateur doivent être réauthentifiées après une interruption de réseau lorsque des clients Horizon utilisent des connexions par tunnel sécurisé vers des postes de travail distants. Lorsque vous sélectionnez ce paramètre, si une connexion par tunnel sécurisé est interrompue, Horizon Client demande à l'utilisateur de se réauthentifier avant la reconnexion. Ce paramètre offre une sécurité améliorée. Par exemple, si un ordinateur portable est volé et déplacé sur un autre réseau, l'utilisateur ne peut pas automatiquement accéder au poste de travail distant sans entrer d'informations d'identification. Lorsque ce paramètre n'est pas sélectionné, le client se reconnecte au poste de travail distant sans demander à l'utilisateur de se réauthentifier. Ce paramètre est sans effet lorsque le tunnel sécurisé n'est pas utilisé.
Mode de sécurité des messages	Détermine le mécanisme de sécurité utilisé pour l'envoi de messages JMS entre composants ■ Lorsque ce mode est défini sur **Activé**, les messages JMS transmis entre des composants View sont signés et vérifiés. ■ Lorsque le mode est défini sur **Amélioré**, la sécurité est fournie par des connexions SSL JMS mutuellement authentifiées et un contrôle d'accès sur les rubriques JMS. Pour plus d'informations, reportez-vous à « Mode de sécurité des messages des composants View », page 35. Pour de nouvelles installations, par défaut, le mode de sécurité des messages est défini sur **Amélioré**. Si vous procédez à une mise à niveau à partir d'une version précédente, le paramètre utilisé dans la version précédente est conservé.
État de sécurité amélioré (lecture seule)	Champ en lecture seule qui s'affiche lorsque **Mode de sécurité des messages** est modifié de **Activé** à **Amélioré**. Comme la modification est effectuée par phases, ce champ montre la progression de l'opération : ■ **En attente du redémarrage du bus de message** est la première phase. Cet état s'affiche jusqu'à ce que vous redémarriez manuellement toutes les instances du Serveur de connexion de l'espace ou le service Composant du bus de message VMware Horizon View sur tous les hôtes de Serveur de connexion de l'espace. ■ **Amélioré en attente** est l'état suivant. Dès que tous les services Composant du bus de messages View ont été redémarrés, le système commence à modifier le mode de sécurité des messages sur **Amélioré** pour tous les postes de travail et serveurs de sécurité. ■ **Amélioré** est l'état final, indiquant que tous les composants utilisent maintenant le mode de sécurité des messages **Amélioré**. Vous pouvez également employer l'utilitaire de ligne de commande `vdmutil` pour surveiller l'avancement. Reportez-vous à la section « Utilisation de l'utilitaire vdmutil pour configurer le mode de sécurité des messages JMS », page 36.
Utiliser IPSec pour les connexions du serveur de sécurité	Détermine s'il est nécessaire d'utiliser IPSec (Internet Protocol Security) pour les connexions entre des serveurs de sécurité et des instances de Serveur de connexion View. Par défaut, les connexions sécurisées (utilisant IPSec) pour les connexions du serveur de sécurité sont activées.

Remarque Si vous procédez à une mise à niveau vers View 5.1 ou version ultérieure à partir d'une version antérieure de View, le paramètre général **Exiger SSL pour les connexions client** s'affiche dans View Administrator, mais seulement si le paramètre a été désactivé dans votre configuration de View avant la mise à niveau. Comme SSL est requis pour toutes les connexions d'Horizon Client et pour les connexions de View Administrator à View, ce paramètre ne s'affiche pas dans les nouvelles installations de View 5.1 ou version ultérieure et n'est pas affiché après une mise à niveau s'il avait déjà été activé dans la configuration précédente de View.

Après une mise à niveau, si vous n'activez pas le paramètre **Exiger SSL pour les connexions client**, les connexions HTTPS à partir des clients Horizon échouent si ces derniers ne se connectent pas à un périphérique intermédiaire qui est configuré pour établir des connexions directes à l'aide de HTTP. Reportez-vous à la section « Décharger des connexions SSL sur des serveurs intermédiaires », page 41.

Mode de sécurité des messages des composants View

Vous pouvez définir le mode de sécurité des messages pour spécifier le mécanisme de sécurité utilisé lorsque des messages JMS sont échangés entre des composants View.

Tableau 2-4 affiche les options que vous pouvez sélectionner pour configurer le mode de sécurité des messages. Pour définir une option, sélectionnez-la dans la liste **Mode de sécurité des messages** dans la boîte de dialogue Paramètres généraux.

Tableau 2-4. Options du mode de sécurité des messages

Option	Description
Désactivé	Le mode de sécurité des messages est désactivé.
Mélangé	Le mode de sécurité des messages est activé mais pas appliqué. Vous pouvez utiliser ce mode pour détecter les composants de votre environnement View qui précèdent View 3.0. Les fichiers journaux générés par le Serveur de connexion View contiennent des références à ces composants. Ce paramètre n'est pas recommandé. Utilisez ce paramètre uniquement pour découvrir les composants devant être mis à niveau.
Activé	Le mode de sécurité des messages est activé, utilisation d'une combinaison de signature et de chiffrement des messages. Les messages JMS sont rejetés si la signature est manquante ou non valide, ou si un message a été modifié après avoir été signé. Certains messages JMS sont chiffrés, car ils comportent des informations sensibles telles que les informations d'identification de l'utilisateur. Si vous utilisez le paramètre **Activé**, vous pouvez également utiliser IPSec pour chiffrer tous les messages JMS entre les instances du Serveur de connexion View, et entre les instances du Serveur de connexion View et les serveurs de sécurité. **Remarque** Les composants de View qui sont antérieurs à View 3.0 ne sont pas autorisés à communiquer avec d'autres composants View.
Amélioré	SSL est utilisé pour toutes les connexions JMS. Le contrôle d'accès JMS est également activé afin que les postes de travail, les serveurs de sécurité et les instances du Serveur de connexion View puissent envoyer et recevoir uniquement des messages JMS sur certaines rubriques. Les composants View antérieurs à Horizon 6 version 6.1 ne peuvent pas communiquer avec une instance de Serveur de connexion View 6.1. **Remarque** L'utilisation de ce mode nécessite l'ouverture du port TCP 4002 entre les serveurs de sécurité basés sur DMZ et leurs instances du Serveur de connexion View couplées.

La première fois que vous installez View sur un système, le mode de sécurité des messages est défini sur **Activé**. Si vous effectuez la mise à niveau de View à partir d'une version précédente, le mode de sécurité des messages reste le même.

Important Si vous prévoyez de modifier un environnement View mis à niveau d'**Activé** à **Amélioré**, vous devez d'abord mettre à niveau toutes les instances du Serveur de connexion View, les serveurs de sécurité et les postes de travail View vers Horizon 6 version 6.1 ou version ultérieure. Dès que vous avez défini le paramètre sur **Amélioré**, le nouveau paramètre entre en vigueur par étapes.

1 Vous devez redémarrer manuellement le service Composant du bus de message VMware Horizon View sur tous les hôtes de Serveur de connexion View de l'espace ou redémarrer les instances de Serveur de connexion View.

2 Dès que les services ont redémarré, les instances du Serveur de connexion View reconfigurent le mode de sécurité des messages sur tous les postes de travail et serveurs de sécurité, pour passer au mode **Amélioré**.

3 Pour surveiller l'avancement dans View Administrator, accédez à **Configuration de View > Paramètres généraux**.

   Dans l'onglet **Sécurité**, l'élément **État de sécurité amélioré** affiche **Amélioré** lorsque tous les composants ont effectué la transition vers le mode Amélioré.

   Sinon, vous pouvez employer l'utilitaire de ligne de commande `vdmutil` pour surveiller l'avancement. Reportez-vous à la section « Utilisation de l'utilitaire vdmutil pour configurer le mode de sécurité des messages JMS », page 36.

Les composants View antérieurs à Horizon 6 version 6.1 ne peuvent pas communiquer avec une instance du Serveur de connexion View 6.1 utilisant le mode Amélioré.

Si vous prévoyez de modifier un environnement View actif de **Désactivé** à **Activé**, ou de **Activé** à **Désactivé**, passez en mode **Mélangé** pendant une courte période avant de faire la modification finale. Par exemple, si votre mode actuel est **Désactivé**, passez en mode **Mélangé** pendant une journée, puis passez à **Activé**. En mode **Mélangé**, 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.

Utilisation de l'utilitaire vdmutil pour configurer le mode de sécurité des messages JMS

Vous pouvez utiliser l'interface de ligne de commande `vdmutil` pour configurer et gérer le mécanisme de sécurité utilisé lorsque des messages JMS sont transmis entre des composants View.

Syntaxe et emplacement de l'utilitaire

La commande `vdmutil` peut effectuer les mêmes opérations que la commande `lmvutil` qui était incluse avec les versions antérieures de View. En outre, la commande `vdmutil` dispose d'options permettant de déterminer le mode de sécurité des messages utilisés et de surveiller l'avancement du passage de tous les composants View en mode Amélioré. Utilisez la forme suivante de la commande `vdmutil` dans une invite de commande Windows.

`vdmutil` *`command_option`* [*`additional_option argument`*] ...

Les options supplémentaires que vous pouvez utiliser dépendent de l'option de commande. Cette rubrique met l'accent sur les options du mode de sécurité des messages. Pour les autres options, liées à Cloud Pod Architecture, reportez-vous au document *Administration d'Architecture Cloud Pod dans Horizon 7*.

Par défaut, le chemin d'accès vers le fichier exécutable de la commande `vdmutil` est `C:\Program Files\VMware\VMware View\Server\tools\bin`. Pour éviter d'entrer le chemin d'accès sur la ligne de commande, ajoutez-le à la variable d'environnement PATH.

Authentification

Vous devez exécuter la commande en tant qu'utilisateur disposant du rôle Administrateurs. Vous pouvez utiliser View Administrator pour attribuer le rôle Administrateurs à un utilisateur. Reportez-vous à la section Chapitre 6, « Configuration d'administration déléguée basée sur des rôles », page 111.

La commande `vdmutil` inclut des options pour spécifier le nom d'utilisateur, le domaine et le mot de passe à utiliser pour l'authentification.

Tableau 2-5. options d'authentification de la commande vdmutil

Option	Description
`--authAs`	Nom d'un utilisateur administrateur View. N'utilisez ni le format *domain**username* ni le format de nom principal d'utilisateur (UPN).
`--authDomain`	Nom de domaine complet de l'utilisateur administrateur View spécifié dans l'option `--authAs`.
`--authPassword`	Mot de passe de l'utilisateur administrateur View spécifié dans l'option `--authAs`. Si vous entrez **« * »** plutôt qu'un mot de passe, la commande `vdmutil` affiche une invite de mot de passe et ne conserve pas les mots de passe sensibles dans l'historique des commandes sur la ligne de commande.

Vous devez utiliser les options d'authentification avec toutes les options de la commande `vdmutil`, à l'exception de `--help` et de `--verbose`.

Options spécifiques aux modes de sécurité des messages JMS

Le tableau suivant répertorie uniquement les options de ligne de commande `vdmutil` qui concernent l'affichage, la configuration ou la surveillance du mode de sécurité des messages JMS. Pour consulter la liste des arguments que vous pouvez utiliser avec une option spécifique, utilisez l'option de ligne de commande `--help`.

La commande `vdmutil` renvoie 0 lorsqu'une opération réussit et un code différent de zéro spécifique d'un échec lorsqu'une opération échoue. La commande `vdmutil` écrit des messages d'erreur en format d'erreur standard. Lorsqu'une opération produit une sortie ou lorsque la journalisation détaillée est activée à l'aide de l'option `--verbose`, la commande `vdmutil` écrit la sortie en format de sortie standard, en anglais américain.

Tableau 2-6. Options de la commande vdmutil

Option	Description
`--activatePendingConnectionServerCertificates`	Active un certificat de sécurité en attente pour une instance du Serveur de connexion View dans l'espace local.
`--countPendingMsgSecStatus`	Compte le nombre de machines empêchant une transition vers ou depuis le mode Amélioré.
`--createPendingConnectionServerCertificates`	Crée un certificat de sécurité en attente pour une instance du Serveur de connexion View dans l'espace local.
`--getMsgSecLevel`	Obtient l'état de sécurité des messages amélioré pour l'espace local. Cet état concerne le processus de changement du mode de sécurité des messages JMS d'**Activé** à **Amélioré** pour tous les composants d'un environnement View.
`--getMsgSecMode`	Obtient le mode de sécurité des messages pour l'espace local.
`--help`	Répertorie les options de la commande `vdmutil`. Vous pouvez également utiliser `--help` sur une commande particulière, comme `--setMsgSecMode --help`.
`--listMsgBusSecStatus`	Répertorie l'état de sécurité du bus de message pour tous les serveurs de connexion de l'espace local.

Tableau 2-6. Options de la commande vdmutil (suite)

Option	Description
`--listPendingMsgSecStatus`	Répertorie les machines empêchant une transition vers ou depuis le mode Amélioré. Limité à 25 entrées par défaut.
`--setMsgSecMode`	Définit le mode de sécurité des messages de l'espace local.
`--verbose`	Active la journalisation détaillée. Vous pouvez ajouter cette option à n'importe quelle autre option pour obtenir une sortie de commande détaillée. La commande `vdmutil` écrit dans la sortie standard.

Configurer le tunnel sécurisé et PCoIP Secure Gateway

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

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

Remarque Avec Horizon 6 version 6.2 et ultérieures, vous pouvez utiliser des dispositifs Access Point, plutôt que des serveurs de sécurité, pour l'accès externe sécurisé vers des serveurs et des postes de travail Horizon 6. Si vous utilisez des dispositifs Access Point, vous devez désactiver les passerelles sécurisées sur les instances du Serveur de connexion View et activer ces passerelles sur les dispositifs Access Point. Pour plus d'informations, consultez le document *Déploiement et configuration d'Access Point*.

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

Important Une configuration de réseau classique qui fournit des connexions sécurisées pour 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 du Serveur de connexion View qui est couplée avec le serveur de sécurité.

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

Prérequis

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

Procédure

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

2 Sur l'onglet **Serveurs de connexion**, sélectionnez une instance de Serveur de connexion View et cliquez sur **Modifier**.

3 Configurez l'utilisation du tunnel sécurisé.

Option	Description
Activer le tunnel sécurisé	Sélectionnez **Utiliser une connexion par tunnel sécurisé à la machine**.
Désactiver le tunnel sécurisé	Désélectionnez **Utiliser une connexion par tunnel sécurisé à la machine**.

Le tunnel sécurisé est activé par défaut.

4 Configurez l'utilisation de PCoIP Secure Gateway.

Option	Description
Activer PCoIP Secure Gateway	Sélectionnez **Utiliser PCoIP Secure Gateway pour les connexions PCoIP à la machine**
Désactiver PCoIP Secure Gateway	Désélectionnez **Utiliser PCoIP Secure Gateway pour les connexions PCoIP à la machine**.

Par défaut, PCoIP Secure Gateway est désactivé.

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

Configurer Blast Secure Gateway

Dans Horizon Administrator, vous pouvez configurer l'utilisation de Blast Secure Gateway pour offrir un accès sécurisé à des applications et des postes de travail distants, via HTML Access ou via des connexions clientes qui utilisent le protocole d'affichage VMware Blast.

Blast Secure Gateway inclut la mise en réseau Blast Extreme Adaptive Transport (BEAT), qui s'ajuste dynamiquement aux conditions du réseau, comme les vitesses variables et les pertes de paquets.

- Les instances d'Horizon Client peuvent utiliser la mise en réseau BEAT avec une excellente condition de réseau lors de la connexion au Serveur de connexion, au serveur de sécurité ou au dispositif Access Point.
- Les instances d'Horizon Client qui utilisent une condition de réseau normale doivent se connecter à un Serveur de connexion (BSG désactivé), un serveur de sécurité (BSG désactivé) ou à des versions ultérieures à la version 2.8 d'un dispositif Access Point. Si Horizon Client utilise une condition de réseau normale pour se connecter à un Serveur de connexion (BSG activé), à un serveur de sécurité (BSG activé) ou à des versions antérieures à la version 2.8 d'un dispositif Access Point, le client détecte automatiquement la condition de réseau et revient à la mise en réseau TCP.
- Les instances d'Horizon Client qui utilisent une condition de réseau faible doivent se connecter à la version 2.9 ou ultérieure d'un dispositif Access Point (avec le serveur tunnel UDP activé). Si Horizon Client utilise une condition de réseau faible pour se connecter à un Serveur de connexion (BSG activé), à un serveur de sécurité (BSG activé) ou à des versions antérieures à la version 2.8 d'un dispositif Access Point, le client détecte automatiquement la condition de réseau et revient à la mise en réseau TCP.
- Pour les instances d'Horizon Client qui utilisent une condition de réseau faible pour se connecter à un Serveur de connexion (BSG désactivé), un serveur de sécurité (BSG désactivé), à la version 2.9 ou ultérieure d'un dispositif Access Point (sans serveur de tunnel UDP activé) ou à la version 2.8 d'un dispositif Access Point, le client détecte automatiquement la condition de réseau et revient à la condition de réseau normale.

Pour plus d'informations, consultez la documentation d'Horizon Client à l'adresse https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

Remarque Vous pouvez également utiliser des dispositifs Access Point, plutôt que des serveurs de sécurité, pour un accès externe sécurisé à des serveurs et des postes de travail Horizon 7. Si vous utilisez des dispositifs Access Point, vous devez désactiver les passerelles sécurisées sur les instances du Serveur de connexion et activer ces passerelles sur les dispositifs Access Point. Pour plus d'informations, consultez le document *Déploiement et configuration d'Access Point*.

Lorsque Blast Secure Gateway n'est pas activé, les périphériques clients et les navigateurs Web clients utilisent le protocole VMware Blast Extreme pour établir des connexions directes à des machines virtuelles de poste de travail distant et à des applications, en contournant 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 du Serveur de connexion couplée avec le serveur de sécurité. Si des utilisateurs externes se connectent directement à un hôte du Serveur de connexion, vous activez ou désactivez Blast Secure Gateway en modifiant cette instance du Serveur de connexion.

Prérequis

Si des utilisateurs sélectionnent des postes de travail distants à l'aide de VMware Identity Manager, vérifiez que VMware Identity Manager est installé et configuré pour être utilisé avec le Serveur de connexion et que ce dernier est couplé avec un serveur d'authentification SAML 2.0.

Procédure

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

2 Dans l'onglet **Serveurs de connexion**, sélectionnez une instance du Serveur de connexion 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 les connexions Blast à la machine**
Désactiver Blast Secure Gateway	Décochez la case **Utiliser Blast Secure Gateway pour les connexions Blast à la machine**

Blast Secure Gateway est activé par défaut.

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

Décharger des connexions SSL sur des serveurs intermédiaires

Horizon Client doit utiliser HTTPS pour se connecter à View. Si vos clients Horizon Client se connectent à des équilibrages de charge ou à d'autres serveurs intermédiaires qui transmettent les connexions à des instances du Serveur de connexion View ou à des serveurs de sécurité, vous pouvez décharger SSL vers les serveurs intermédiaires.

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

Si vous déchargez des connexions SSL vers un serveur intermédiaire, vous devez importer le certificat du serveur intermédiaire vers les instances du Serveur de connexion View ou les serveurs de sécurité qui se connectent au serveur intermédiaire. Le même certificat de serveur SSL doit résider sur le serveur intermédiaire de déchargement et sur chaque serveur View déchargé qui se connecte au serveur intermédiaire.

Si vous déployez des serveurs de sécurité, le serveur intermédiaire et les serveurs de sécurité qui s'y connectent doivent avoir le même certificat SSL. Vous n'avez pas à installer le même certificat SSL sur les instances du Serveur de connexion View qui sont couplées aux serveurs de sécurité et ne se connectent pas directement au serveur intermédiaire.

Si vous ne déployez pas de serveurs de sécurité ou si vous avez un environnement réseau mélangé avec des serveurs de sécurité et des instances du Serveur de connexion View frontales externes, le serveur intermédiaire et les instances du Serveur de connexion View qui s'y connectent doivent avoir le même certificat SSL.

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

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 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 périphériques Horizon Client utilisent le tunnel sécurisé pour se connecter à View, vous devez définir l'URL externe du tunnel sécurisé sur une adresse que les clients peuvent utiliser pour accéder 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.

Si vous déployez des serveurs de sécurité, des URL externes sont requises pour les serveurs de sécurité mais pas pour les instances de Serveur de connexion View qui sont couplées avec les serveurs de sécurité.

Si vous ne déployez pas de serveurs de sécurité ou si vous disposez d'un environnement réseau mixte comportant des serveurs de sécurité et des instances de Serveur de connexion View externes, des URL externes sont requises pour les instances du Serveur de connexion View qui se connectent au serveur intermédiaire.

Remarque Vous ne pouvez pas décharger des connexions SSL à partir d'un composant PCoIP Secure Gateway (PSG) ou Blast Secure Gateway. L'URL externe de PCoIP et l'URL externe de Blast Secure Gateway doivent permettre aux clients de se connecter à l'ordinateur qui héberge PSG et Blast Secure Gateway. Ne réinitialisez pas l'URL externe de PCoIP et l'URL externe de Blast pour pointer vers le serveur intermédiaire sauf si vous prévoyez d'exiger des connexions SSL entre le serveur intermédiaire et View Server.

Pour plus d'informations sur la configuration des URL externes, reportez-vous à « Configuration d'URL externes pour PCoIP Secure Gateway et les connexions de tunnel » dans le document *Installation de View*.

Autoriser les connexions HTTP à partir des serveurs intermédiaires

Quand le certificat SSL est déchargé vers un serveur intermédiaire, vous pouvez configurer les instances du Serveur de connexion View ou les serveurs de sécurité pour autoriser les connexions HTTP à partir des périphériques intermédiaires clients. Les périphériques intermédiaires doivent accepter HTTPS pour les connexions d'Horizon Client.

Pour autoriser les connexions HTTP entre les serveurs View et les périphériques intermédiaires, vous devez configurer le fichier `locked.properties` sur chaque instances du Serveur de connexion View et le serveur de sécurité sur lequel les connexions HTTP sont autorisées.

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

Remarque Si vos clients Horizon utilisent l'authentification par carte à puce, ils doivent établir des connexions HTTPS directement avec le Serveur de connexion View ou le serveur de sécurité. Le déchargement SSL n'est pas prise 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 du 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 du serveur View, ajoutez la propriété `serverProtocol` et définissez-la sur `http`.

   La valeur `http` doit être tapée en minuscules.

3 (Facultatif) Ajoutez des propriétés pour configurer un port d'écoute HTTP qui n'est pas par défaut et une interface réseau sur le serveur View.

   - Pour modifier le port d'écoute HTTP 80, définissez `serverPortNonSSL` sur un autre numéro de port sur lequel le périphérique intermédiaire est configuré pour se connecter.
   - Si le serveur View dispose de plus d'une interface réseau et que vous prévoyez que le serveur écoute les connexions HTTP sur une seule interface, définissez `serverHostNonSSL` sur 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 autorise les connexions HTTP non-SSL à un serveur View. L'adresse IP de l'interface réseau cliente du serveur View est 10.20.30.40. Le serveur utilise le port 80 par défaut pour écouter les connexions HTTP. La valeur `http` doit être en minuscules.

```
serverProtocol=http
serverHostNonSSL=10.20.30.40
```

Configurer l'emplacement de la passerelle pour un hôte du Serveur de connexion Horizon ou du serveur de sécurité

Par défaut, les instances du Serveur de connexion Horizon définissent l'emplacement de la passerelle sur `Interne` et les serveurs de sécurité définissent l'emplacement de la passerelle sur `Externe`. Vous pouvez modifier l'emplacement par défaut de la passerelle en définissant la propriété `gatewayLocation` dans le fichier `locked.properties`.

L'emplacement de la passerelle détermine la valeur de clé de registre `ViewClient_Broker_GatewayLocation` dans un poste de travail distant. Vous pouvez utiliser cette valeur avec des stratégies de carte à puce pour créer une stratégie qui ne prend effet que si un utilisateur se connecte à un poste de travail distant à l'intérieur ou à l'extérieur du réseau d'entreprise. Pour plus d'informations, consultez « Utilisation de stratégies de carte à puce » dans le document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

Procédure

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

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

   Les propriétés dans le fichier `locked.properties` sont sensibles à la casse.

2. Ajoutez la ligne suivante au fichier `locked.properties` :

   `gatewayLocation=`*`value`*

   value peut être `Externe` ou `Interne`. `Externe` indique que la passerelle est disponible pour les utilisateurs à l'extérieur du réseau d'entreprise. `Interne` indique que la passerelle est disponible pour les utilisateurs à l'intérieur du réseau d'entreprise.

   Par exemple : `gatewayLocation=External`

3. Enregistrez le fichier `locked.properties`.
4. Redémarrez le service Serveur de connexion VMware Horizon ou le service du serveur de sécurité VMware Horizon pour que vos modifications prennent effet.

Désactiver ou activer le Serveur de connexion View

Vous pouvez désactiver une instance du Serveur de connexion View pour empêcher les utilisateurs de se connecter à leurs applications et postes de travail distants. Après avoir désactivé une instance, vous pouvez l'activer de nouveau.

Lorsque vous désactivez une instance du Serveur de connexion View, les utilisateurs actuellement connectés à des applications et des postes de travail distants ne sont pas affectés.

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

- S'il s'agit d'une instance autonome du Serveur de connexion View, les utilisateurs ne peuvent pas se connecter à leurs applications ou postes de travail distants. Ils ne peuvent pas se connecter au Serveur de connexion View.

- S'il s'agit d'une instance du Serveur de connexion View 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 se connecter à leurs applications et postes de travail distants.

Procédure

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

2 Dans l'onglet **Serveurs de connexion**, sélectionnez l'instance du Serveur de connexion View.

3 Cliquez sur **Désactiver**.

Vous pouvez activer de nouveau l'instance en cliquant sur **Activer**.

Modifier les URL externes

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

Par défaut, un hôte du 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 du Serveur de connexion View ou du serveur de sécurité.

Lorsque des utilisateurs se connectent à des postes de travail distants avec le protocole d'affichage PCoIP, Horizon Client peut établir une autre connexion à PCoIP Secure Gateway sur l'hôte du 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 du Serveur de connexion View ou du serveur de sécurité. Vous spécifiez cette adresse IP dans l'URL externe PCoIP.

Une troisième URL permet aux utilisateurs de faire des connexions sécurisées via Blast Secure Gateway.

L'URL externe de tunnel sécurisé, l'URL externe PCoIP et l'URL externe Blast doivent être les adresses que les systèmes clients utilisent pour atteindre cet hôte.

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, sélectionnez **Configuration de View > Serveurs**.

Option	Action
Instance de Serveur de connexion View	Dans l'onglet **Serveurs de connexion**, sélectionnez l'instance du Serveur de connexion View et cliquez sur **Modifier**.
Serveur de sécurité	Sélectionnez le serveur de sécurité dans l'onglet **Serveurs de sécurité**, puis cliquez sur **Modifier**.

2 Saisissez l'URL externe du tunnel sécurisé dans la zone de texte **URL externe**.

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

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

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

3 Saisissez l'URL externe de PCoIP Secure Gateway dans la zone de texte **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 du Serveur de connexion View.

4 Saisissez l'URL externe Blast Secure Gateway dans la zone de texte **URL externe Blast**.

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

Par exemple : `https://myserver.example.com:8443`

Par défaut, l'URL inclut le nom de domaine complet de l'URL externe du tunnel sécurisé et le numéro de port par défaut, 8443. L'URL doit contenir le nom de domaine complet et le numéro de port qu'un système client peut utiliser pour atteindre cet hôte.

5 Vérifiez que toutes les adresses de cette boîte de dialogue permettent aux systèmes clients d'atteindre cet hôte.

6 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'expérience utilisateur

Lorsque vous installez le Serveur de connexion View avec une nouvelle configuration, vous avez la possibilité de participer à un programme d'amélioration de l'expérience utilisateur. Si vous changez d'avis après l'installation, vous pouvez vous participer au programme ou vous en retirer à l'aide de View Administrator.

Si vous participez au programme, VMware collecte des données anonymes sur votre déploiement afin d'améliorer sa réponse aux besoins de ses utilisateurs. Aucune donnée permettant d'identifier votre organisation n'est collectée.

Pour vérifier la liste des champs auprès desquels les données sont collectées, ainsi que ceux qui sont anonymes, reportez-vous à

« Informations collectées par le programme d'amélioration de l'expérience utilisateur », page 162.

Procédure

1 Dans View Administrator, sélectionnez **Configuration de View > Licence produit et utilisation**.

2 Dans le volet Programme d'expérience utilisateur, cliquez sur **Modifier les paramètres**.

3 Indiquez si vous souhaitez participer ou vous retirer du programme en cochant ou en décochant la case **Envoyer des données anonymes à VMware**.

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

5 Cliquez sur **OK**.

Répertoire View LDAP

View LDAP est le référentiel de données de l'ensemble des informations de configuration de View. View LDAP est un répertoire LDAP (Lightweight Directory Access Protocol) incorporé fourni avec l'installation du Serveur de connexion View.

View LDAP contient les composants d'annuaire LDAP standard utilisés par View :

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

View LDAP contient des entrées d'annuaire qui représentent des objets View.

- Des entrées de poste de travail distant 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 distants qui représentent plusieurs postes de travail gérés ensemble
- Des entrées de machines virtuelles qui représentent la machine virtuelle vCenter Server de chaque poste de travail distant
- Des entrées de composants View qui stockent des paramètres de configuration

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

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

Réplication LDAP

Lorsque vous installez une instance répliquée du Serveur de connexion View, View copie les données de configuration View LDAP depuis l'instance du Serveur de connexion View existante. Les données de configuration de View LDAP identiques sont conservées sur toutes les instances du Serveur de connexion View du groupe répliqué. Lorsqu'une modification est faite sur une instance, les informations mises à jour sont copiées sur les autres instances.

Si une instance répliquée échoue, les autres instances du groupe continuent de fonctionner. Lorsque l'instance échouée reprend l'activité, sa configuration est mise à jour avec les modifications qui ont eu lieu au cours de la panne. Avec Horizon 7 et versions ultérieures, une vérification de l'état de réplication est effectuée toutes les 15 minutes pour déterminer si chaque instance peut communiquer avec les autres serveurs dans le groupe répliqué et si chaque instance peut extraire des mises à jour LDAP depuis les autres serveurs dans le groupe.

Vous pouvez utiliser le tableau de bord dans View Administrator pour vérifier l'état de réplication. Si des instances du Serveur de connexion View ont une icône rouge dans le tableau de bord, cliquez sur l'icône pour voir l'état de réplication. La réplication peut être affectée pour l'une des raisons suivantes :

- Un pare-feu peut bloquer la communication
- Le service VDMDS de VMware peut être arrêté pour une instance du Serveur de connexion View
- Les options VDMDS DSA de VMware peuvent bloquer les réplications
- Un problème de réseau s'est produit

Par défaut, la vérification de la réplication a lieu toutes les 15 minutes. Vous pouvez utiliser l'Éditeur ADSI sur une instance du Serveur de connexion View pour modifier l'intervalle. Pour définir le nombre de minutes, connectez-vous à **DC=vdi,DC=vmware,DC=int** et modifiez l'attribut **pae-ReplicationStatusDataExpiryInMins** sur l'objet **CN=Common,OU=Global,OU=Properties**.

La valeur de l'attribut **pae-ReplicationStatusDataExpiryInMins** doit être comprise entre 10 et 1 440 minutes (un jour). Si la valeur d'attribut est inférieure à 10 minutes, View la traite comme si elle était égale à 10 minutes. Si la valeur d'attribut est supérieure à 1 440, View la traite comme si elle était égale à 1 440 minutes.

Configuration de l'authentification par carte à puce 3

Pour une sécurité accrue, vous pouvez configurer une instance du Serveur de connexion View ou un serveur de sécurité de sorte que les utilisateurs et les administrateurs puissent s'authentifier par carte à puce.

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. Un type de carte à puce utilisé par le Département de la Défense des États-Unis se nomme carte CAC (Common Access Card).

Avec l'authentification par carte à puce, un utilisateur ou un administrateur insère une carte à puce dans un lecteur de carte à puce connecté à l'ordinateur client et entre un code PIN. L'authentification par carte à puce fournit une authentification à deux facteurs en vérifiant à la fois ce que la personne a (la carte à puce) et ce qu'elle sait (le code PIN).

Pour plus d'informations sur les configurations matérielles et logicielles requises pour l'implémentation de l'authentification par carte à puce, reportez-vous au document *Installation de 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.

Pour utiliser des cartes à puce, des machines client doivent comporter un intergiciel de carte à puce et un lecteur de carte à puce. Pour installer des certificats sur des cartes à puce, vous devez configurer un ordinateur afin qu'il agisse comme station d'inscription. Pour déterminer si un type particulier de Horizon Client prend en charge les cartes à puce, reportez-vous à la documentation de Horizon Client à l'adresse https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

Ce chapitre aborde les rubriques suivantes :

Ouverture de session avec une carte à puce

Lorsqu'un utilisateur ou un administrateur insère une carte à puce dans un lecteur de carte à puce, les certificats utilisateur de la carte à puce sont copiés dans le magasin de certificats local sur le système client si son système d'exploitation est Windows. Les certificats dans le magasin de certificats local sont disponibles pour toutes les applications exécutées sur l'ordinateur client, y compris Horizon Client.

Lorsqu'un utilisateur ou un administrateur initie une connexion à une instance du Serveur de connexion View ou à un serveur de sécurité configuré pour l'authentification par carte à puce, l'instance du Serveur de connexion View ou le serveur de sécurité envoie une liste d'autorités de certification approuvées au système client. Le système client compare cette liste aux certificats utilisateur disponibles, sélectionne un certificat approprié et invite l'utilisateur ou l'administrateur à entrer un code PIN de carte à puce. Si plusieurs certificats utilisateur sont valides, le système client invite l'utilisateur ou l'administrateur à sélectionner un certificat.

Le système client envoie le certificat utilisateur à l'instance du Serveur de connexion View ou au serveur de sécurité, qui vérifie le certificat en contrôlant l'approbation du certificat et sa période de validité. En général, les utilisateurs et les administrateurs peuvent s'authentifier si leur certificat utilisateur est signé et valide. Si la vérification de la révocation des certificats est configurée, les utilisateurs ou les administrateurs dont les certificats utilisateur sont révoqués ne peuvent pas s'authentifier.

Dans certains environnements, le certificat de carte à puce d'un utilisateur peut effectuer un mappage vers plusieurs comptes d'utilisateur de domaine Active Directory. Un utilisateur peut disposer de plusieurs comptes avec des privilèges d'administrateur et doit spécifier quel compte utiliser dans le champ Conseil de nom d'utilisateur lors de la connexion par carte à puce. Pour que le champ Conseil de nom d'utilisateur apparaisse dans la boîte de dialogue de connexion d'Horizon Client, l'administrateur doit activer la fonctionnalité de conseils de nom d'utilisateur de carte à puce pour l'instance du Serveur de connexion dans View Administrator. L'utilisateur de carte à puce peut entrer un nom d'utilisateur ou un UPN dans le champ Conseil de nom d'utilisateur lors de la connexion par carte à puce.

Si votre environnement utilise un dispositif Access Point pour sécuriser l'accès externe, vous devez configurer ce dispositif afin qu'il prenne en charge la fonctionnalité de conseils de nom d'utilisateur de carte à puce. La fonctionnalité de conseils de nom d'utilisateur de carte à puce n'est prise en charge qu'avec Access Point 2.7.2 et versions ultérieures. Pour plus d'informations sur l'activation de la fonctionnalité de conseils de nom d'utilisateur de carte à puce dans Access Point, consultez le document *Déploiement et configuration d'Access Point*.

Le changement du protocole d'affichage n'est pas pris en charge avec l'authentification par carte à puce dans Horizon Client. Pour modifier les protocoles d'affichage après une authentification par carte à puce dans Horizon Client, un utilisateur doit fermer puis rouvrir la session.

Configurer l'authentification par carte à puce sur le Serveur de connexion View

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 du Serveur de connexion View 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 des certificats d'autorités de certification page 51

Vous devez obtenir tous les certificats d'autorités de certification applicables pour tous les certificats d'utilisateurs de confiance des cartes à puces présentées par vos utilisateurs et administrateurs. Ces certificats incluent des certificats racines et peuvent inclure des certificats intermédiaires si le certificat de carte à puce de l'utilisateur a été délivré par une autorité de certification intermédiaire.

2 Obtenir le certificat d'une autorité de certification de Windows page 52

Si vous disposez d'un certificat utilisateur signé par une autorité de certification ou d'une carte à puce en contenant un, et que Windows approuve le certificat racine, vous pouvez exporter ce dernier de Windows. Si l'émetteur du certificat de l'utilisateur est une autorité de certification intermédiaire, il est possible d'exporter ce certificat.

3 Ajouter le certificat de l'autorité de certification à un fichier du magasin d'approbations du serveur page 52

Vous devez ajouter des certificats racines, intermédiaires ou les deux types à un fichier du magasin d'approbations du serveur pour tous les utilisateurs et administrateurs de confiance. Les instances du Serveur de connexion View et les serveurs de sécurité utilisent ces informations pour authentifier les utilisateurs et les administrateurs de cartes à puce.

4 Modifier des propriétés de configuration du Serveur de connexion View page 53

Pour activer l'authentification par carte à puce, vous devez modifier les propriétés de configuration Serveur de connexion View sur votre hôte du Serveur de connexion View ou du serveur de sécurité.

5 Configurer des paramètres de carte à puce dans View Administrator page 54

Vous pouvez utiliser View Administrator pour spécifier des paramètres afin de s'adapter à différents scénarios d'authentification par carte à puce.

Obtenir des certificats d'autorités de certification

Vous devez obtenir tous les certificats d'autorités de certification applicables pour tous les certificats d'utilisateurs de confiance des cartes à puces présentées par vos utilisateurs et administrateurs. Ces certificats incluent des certificats racines et peuvent inclure des certificats intermédiaires si le certificat de carte à puce de l'utilisateur a été délivré par une autorité de certification intermédiaire.

Si vous ne disposez pas du certificat racine ou intermédiaire de l'autorité de certification qui a signé les certificats sur les cartes à puce présentées par vos utilisateurs et administrateurs, vous pouvez exporter les certificats à partir des certificats d'utilisateurs signés par une autorité de certification ou d'une carte à puce qui en contient un. Reportez-vous à la section « Obtenir le certificat d'une autorité de certification de Windows », page 52.

Procédure

- Obtenez les certificats d'autorités de certification 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.

Suivant

Ajoutez le certificat racine, le certificat intermédiaire ou les deux à un fichier du magasin d'approbations du serveur.

Obtenir le certificat d'une autorité de certification de Windows

Si vous disposez d'un certificat utilisateur signé par une autorité de certification ou d'une carte à puce en contenant un, et que Windows approuve le certificat racine, vous pouvez exporter ce dernier de Windows. Si l'émetteur du certificat de l'utilisateur est une autorité de certification intermédiaire, il est possible d'exporter ce certificat.

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. Ce fichier est utilisé à l'étape 4 de cette procédure.

2 Dans Internet Explorer, sélectionnez **Outils > Options Internet**.

3 Sous l'onglet **Contenu**, cliquez sur **Certificats**.

4 Sous l'onglet **Personnel**, sélectionnez le certificat que vous voulez utiliser et cliquez sur **Affichage**.

Si le certificat utilisateur n'apparaît pas dans la liste, cliquez sur **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 **Chemin d'accès de certification**, sélectionnez le certificat en haut de l'arborescence et cliquez sur **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. Dans certains cas, l'émetteur peut être une autorité de certification intermédiaire.

6 Sous l'onglet **Détails**, cliquez sur **Copier dans un fichier**.

L'assistant Certificate Export (Exportation de certificat) apparaît.

7 Cliquez sur **Suivant > Suivant**, puis tapez un nom et un emplacement pour le fichier à exporter.

8 Cliquez sur **Suivant** pour enregistrer le fichier comme certificat racine dans l'emplacement spécifié.

Suivant

Ajoutez le certificat de l'autorité de certification à un fichier du magasin d'approbations du serveur.

Ajouter le certificat de l'autorité de certification à un fichier du magasin d'approbations du serveur

Vous devez ajouter des certificats racines, intermédiaires ou les deux types à un fichier du magasin d'approbations du serveur pour tous les utilisateurs et administrateurs de confiance. Les instances du Serveur de connexion View et les serveurs de sécurité utilisent ces informations pour authentifier les utilisateurs et les administrateurs de cartes à puce.

Prérequis

- Vous devez obtenir les certificats racines ou intermédiaires utilisés pour signer les certificats sur les cartes à puce présentées par vos utilisateurs ou administrateurs. Reportez-vous aux sections « Obtenir des certificats d'autorités de certification », page 51 et « Obtenir le certificat d'une autorité de certification de Windows », page 52.

Important Ces certificats peuvent inclure des certificats intermédiaires si le certificat de carte à puce de l'utilisateur a été délivré par une autorité de certification intermédiaire.

- Vérifiez que l'utilitaire `keytool` est ajouté au chemin d'accès du système sur votre hôte du Serveur de connexion View ou du serveur de sécurité. Consultez le document *Installation de View* pour plus d'informations.

Procédure

1 Sur votre hôte du Serveur de connexion View ou du serveur de sécurité, utilisez l'utilitaire `keytool` pour importer le certificat racine, le certificat intermédiaire ou les deux 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 sensible à la casse d'une nouvelle entrée dans le fichier du magasin d'approbations, *root_certificate* est le certificat racine ou intermédiaire que vous avez obtenu ou exporté, et *truststorefile.key* est le nom du 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 du 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 du Serveur de connexion View pour activer l'authentification par carte à puce.

Modifier des propriétés de configuration du Serveur de connexion View

Pour activer l'authentification par carte à puce, vous devez modifier les propriétés de configuration Serveur de connexion View sur votre hôte du Serveur de connexion View ou du serveur de sécurité.

Prérequis

Ajoutez les certificats de l'autorité de certification pour tous les certificats utilisateur approuvés à un fichier du magasin d'approbations du serveur. Ces certificats incluent des certificats racines et peuvent inclure des certificats intermédiaires si le certificat de carte à puce de l'utilisateur a été délivré par une autorité de certification intermédiaire.

Procédure

1 Créez ou modifiez le fichier `locked.properties` dans le dossier de configuration de la passerelle SSL sur l'hôte du 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 affiché 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 de certificat.

```
trustKeyfile=lonqa.key
trustStoretype=jks
useCertAuth=true
```

Suivant

Si vous avez configuré l'authentification par carte à puce pour une instance du 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 sur une instance du Serveur de connexion View s'appliquent également 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 configurez ces paramètres sur une instance du Serveur de connexion View, ils sont également appliqués aux serveurs de sécurité couplés.

Prérequis

- Modifiez les propriétés de configuration du Serveur de connexion View sur votre hôte du Serveur de connexion View.
- Vérifiez qu'Horizon Client établit des connexions HTTPS directement à votre hôte du 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 sur un périphérique intermédiaire.

Procédure

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

2 Dans l'onglet **Serveurs de connexion**, sélectionnez l'instance du Serveur de connexion View et cliquez sur **Modifier**.

3 Pour configurer l'authentification par carte à puce pour les utilisateurs d'applications et de postes de travail distants, procédez comme suit.

a Dans l'onglet **Authentification**, sélectionnez une option de configuration dans le menu déroulant **Authentification par carte à puce** de la section Authentification de View.

Option	Action
Non autorisée	L'authentification par carte à puce est désactivée sur l'instance du Serveur de connexion View.
Facultative	Les utilisateurs peuvent utiliser l'authentification par carte à puce ou l'authentification par mot de passe pour se connecter à l'instance du 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 du Serveur de connexion View. Lorsque l'authentification par carte à puce est requise, l'authentification échoue pour les utilisateurs qui cochent la case **Se connecter en tant qu'utilisateur actuel** lorsqu'ils se connectent à l'instance du Serveur de connexion View. Ces utilisateurs doivent se réauthentifier avec leur carte à puce et leur code PIN lorsqu'ils ouvrent une session sur le Serveur de connexion View.

Option	Action
	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.

b 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 **Non autorisée**.

Option	Action
Déconnecter des utilisateurs du Serveur de connexion View lorsqu'ils retirent leurs cartes à puce.	Cochez la case **Déconnecter les sessions utilisateur lors du retrait de la carte à puce**.
Laisser les utilisateurs connectés au Serveur de connexion View lorsqu'ils retirent leur carte à puce et les laisser démarrer de nouvelles sessions de poste de travail ou d'application sans se réauthentifier.	Décochez la case **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 du Serveur de connexion View lorsque la case **Se connecter en tant qu'utilisateur actuel** est cochée, même s'ils ouvrent une session sur leur système client avec une carte à puce.

c Configurer la fonctionnalité de conseils de nom d'utilisateur de carte à puce.

Vous ne pouvez pas configurer la fonctionnalité de conseils de nom d'utilisateur de carte à puce lorsque l'authentification par carte à puce est définie sur **Non autorisée**.

Option	Action
Autoriser les utilisateurs à utiliser un seul certificat de carte à puce pour s'authentifier sur plusieurs comptes d'utilisateur.	Cochez la case **Autoriser les conseils de nom d'utilisateur de carte à puce**.
Empêcher les utilisateurs d'utiliser un seul certificat de carte à puce pour s'authentifier sur plusieurs comptes d'utilisateur.	Décochez la case **Autoriser les conseils de nom d'utilisateur de carte à puce**.

4 Pour configurer l'authentification par carte à puce pour la connexion des administrateurs dans View Administrator, cliquez sur l'onglet **Authentification** et sélectionnez une option de configuration dans le menu déroulant **Authentification par carte à puce des administrateurs** dans la section Authentification de l'administration de View.

Option	Action
Non autorisée	L'authentification par carte à puce est désactivée sur l'instance du Serveur de connexion View.
Facultative	Les administrateurs peuvent utiliser l'authentification par carte à puce ou l'authentification par mot de passe pour se connecter à View Administrator. Si l'authentification par carte à puce échoue, l'administrateur doit fournir un mot de passe.
Requis	Les administrateurs doivent utiliser une authentification par carte à puce lorsqu'ils se connectent à View Administrator.

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 modifier les paramètres d'authentification par carte à puce entre **Facultative** et **Requise** sans qu'il soit nécessaire de redémarrer le service Serveur de connexion View.

Les utilisateurs et les administrateurs actuellement connectés ne sont pas affectés par les modifications des 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 58.

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 61.

Configurer l'authentification par carte à puce sur des solutions tierces

Les solutions tierces telles que les équilibrages de charge et les passerelles peuvent exécuter l'authentification par carte à puce en transmettant une assertion SAML qui contient le certificat X.590 et le code PIN crypté de la carte à puce.

Cette rubrique indique les tâches impliquées dans la configuration de solutions tierces afin de fournir le certificat X.590 approprié au Serveur de connexion View une fois qu'il a été validé par le périphérique partenaire. Comme cette fonctionnalité utilise l'authentification SAML, l'une des tâches consiste à créer un authentificateur SAML dans View Administrator.

Pour plus d'informations sur la configuration de l'authentification par carte à puce sur Access Point, consultez le document *Déploiement et configuration d'Access Point*.

Procédure

1 Créez un authentificateur SAML pour la passerelle ou l'équilibrage de charge tiers.

Reportez-vous à la section « Configurer un authentificateur SAML dans View Administrator », page 72.

2 Étendez la période d'expiration des métadonnées du Serveur de connexion View pour que les sessions à distance ne se terminent pas après seulement 24 heures.

Reportez-vous à la section « Modifier la période d'expiration des métadonnées du fournisseur de services sur le Serveur de connexion View », page 75.

3 Si nécessaire, configurez le périphérique tiers afin d'utiliser les métadonnées de fournisseur de service du Serveur de connexion View.

Consultez la documentation produit du périphérique tiers.

4 Configurez les paramètres de la carte à puce sur le périphérique tiers.

Consultez la documentation produit du périphérique tiers.

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 58

  Comme les ouvertures de session par carte à puce reposent sur des noms d'utilisateur principaux (UPN), les comptes d'utilisateurs et d'administrateurs 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 59

  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 racines de confiance page 59

  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 Autorités de certification racines 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 60

  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 et d'administrateurs 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 **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 racines 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 Autorités de certification racines 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, accédez au 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 Sous l'onglet **Stratégie de groupe**, cliquez sur **Ouvrir** pour ouvrir le plug-in 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 **Configuration ordinateur** et ouvrez le dossier **Paramètres Windows\Paramètres de sécurité\Clé publique**.

3 Cliquez avec le bouton droit sur **Autorités de certification racines de confiance** et sélectionnez **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 60.

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, accédez au 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 Sous l'onglet **Stratégie de groupe**, cliquez sur **Ouvrir** pour ouvrir le plug-in 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 **Configuration ordinateur** et ouvrez la stratégie de **Paramètres Windows\Paramètres de sécurité\Clé publique**.

3 Cliquez avec le bouton droit sur **Autorités de certification intermédiaires** et sélectionnez **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 dispose d'un intergiciel pour carte à puce, d'une carte à puce avec un certificat valide et d'un lecteur de carte à puce. Pour ce qui est utilisateurs finaux, vérifiez qu'ils disposent d'Horizon Client.

  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 **Démarrer > Paramètres > Panneau de configuration > Options Internet > Contenu > Certificats > Personnel** afin de vérifier que des certificats sont disponibles pour l'authentification par carte à puce.

  Lorsqu'un utilisateur ou un administrateur insère une carte à puce dans le lecteur prévu à cet effet, Windows copie les certificats de la carte à puce sur l'ordinateur de l'utilisateur. Les applications du système client, notamment Horizon Client, peuvent utiliser ces certificats.

- Dans le fichier `locked.properties` sur l'hôte du Serveur de connexion View ou du serveur de sécurité, vérifiez que la propriété `useCertAuth` est définie sur **`true`** et qu'elle est bien orthographiée.

  Le fichier `locked.properties` se trouve 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 du Serveur de connexion View, vérifiez le paramètre d'authentification par carte à puce dans View Administrator.

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

  b Dans l'onglet **Serveurs de connexion**, sélectionnez l'instance du Serveur de connexion View et cliquez sur **Modifier**.

  c Si vous avez configuré l'authentification par carte à puce pour les utilisateurs, dans l'onglet **Authentification**, vérifiez que l'option **Authentification par carte à puce des utilisateurs** est définie sur **Facultative** ou **Requise**.

  d Si vous avez configuré l'authentification par carte à puce pour les administrateurs, dans l'onglet **Authentification**, vérifiez que l'option **Authentification par carte à puce des administrateurs** est définie sur **Facultative** ou **Requise**.

  Vous devez redémarrer le service Serveur de connexion View 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 **Démarrer > Outils d'administration > Utilisateurs et ordinateurs Active Directory**.

  c Cliquez avec le bouton droit sur le dossier **Utilisateurs** et sélectionnez **Propriétés**.

  L'UPN s'affiche dans les zones de texte **Nom d'ouverture de session de l'utilisateur** de l'onglet **Compte**.

- Si des utilisateurs de carte à puce choisissent le protocole PCoIP ou VMware Blast pour se connecter à des postes de travail à session unique, vérifiez que le composant View Agent ou Horizon Agent appelé Redirection de carte à puce est installé sur les machines mono-utilisateur. La fonctionnalité de carte à puce permet aux utilisateurs de se connecter à des postes de travail à session unique avec des cartes à puce. Les hôtes RDS, sur lesquels le rôle des services Bureau à distance (RDS) est installé, prennent automatiquement en charge la fonctionnalité de carte à puce et vous n'avez donc pas besoin d'installer celle-ci.
- Vérifiez que les fichiers journaux dans *lecteur*`:\Documents and Settings\All Users\Application Data\VMware\VDM\logs` sur l'hôte du Serveur de connexion View 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 du Serveur de connexion View ou sur un serveur de sécurité. Lorsqu'une instance du Serveur de connexion View 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 du Serveur de connexion View ou l'hôte du serveur de sécurité.

Vous pouvez configurer la CRL et OCSP sur la même instance du Serveur de connexion View 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 63

  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 63

  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 63

  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 64

  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 65

  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 65.

Procédure

1 Créez ou modifiez le fichier `locked.properties` dans le dossier de configuration de la passerelle SSL sur l'hôte du 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 `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 65.

Procédure

1 Créez ou modifiez le fichier `locked.properties` dans le dossier de configuration de la passerelle SSL sur l'hôte du 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 `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 3-1 répertorie les propriétés du fichier `locked.properties` concernant la vérification de la révocation des certificats.

Tableau 3-1. 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`**.

Configuration d'autres types d'authentification utilisateur 4

View utilise votre infrastructure Active Directory existante pour l'authentification et la gestion des utilisateurs et des administrateurs. Vous pouvez également intégrer View à d'autres formes d'authentification en plus des cartes à puce, telles que des solutions d'authentification biométrique ou à deux facteurs, comme RSA SecurID et RADIUS, pour authentifier des utilisateurs d'applications et de postes de travail distants.

Ce chapitre aborde les rubriques suivantes :

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).

- La prise en charge de RADIUS offre une large gamme d'autres options d'authentification à deux facteurs basée sur des jetons.
- View fournit également une interface d'extension standard ouverte pour permettre aux fournisseurs de solutions tiers d'intégrer des extensions d'authentification avancées dans 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 applications et à des postes de travail distants de l'extérieur du réseau d'entreprise, sur Internet.

View est certifié par le programme RSA SecurID Ready et prend en charge l'ensemble des fonctionnalités SecurID, notamment New PIN Mode, Next Token Code Mode, RSA Authentication Manager et l'équilibrage de charge.

Ouvrir une session avec l'authentification à deux facteurs

Lorsqu'un utilisateur se connecte à une instance du Serveur de connexion View sur laquelle l'authentification RSA SecurID ou RADIUS est activée, une boîte de dialogue d'ouverture de session RSA SecurID spéciale s'affiche dans Horizon Client.

Les utilisateurs entrent leur nom d'utilisateur et leur code secret d'authentification RSA SecurID ou RADIUS dans la boîte de dialogue d'ouverture de session spéciale. Un code secret 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 de la connexion à View, l'authentification RADIUS fonctionne de la même manière que RSA SecurID. Si le serveur RADIUS émet un challenge d'accès, Horizon Client affiche une boîte de dialogue semblable à l'invite RSA SecurID pour obtenir le code de jeton suivant. Actuellement la prise en charge des challenges RADIUS est limitée à une invite d'entrée de texte. Aucun texte de challenge envoyé par le serveur RADIUS ne s'affiche. Les formes de challenge plus complexes, telles qu'un choix multiple et une sélection d'images, ne sont actuellement pas prises en charge.

  Dès que l'utilisateur a entré les informations d'identification dans Horizon Client, le serveur RADIUS peut envoyer à son téléphone mobile un message texte SMS, un e-mail ou un texte à l'aide d'un autre mécanisme hors bande, contenant un code. L'utilisateur peut entrer ce texte et ce code dans Horizon Client pour terminer l'authentification.
- Comme certains fournisseurs RADIUS offrent la possibilité d'importer des utilisateurs d'Active Directory, les utilisateurs finaux peuvent d'abord être invités à fournir des informations d'identification Active Directory avant d'entrer un nom d'utilisateur et un code secret d'authentification RADIUS.

Activer l'authentification à deux facteurs dans View Administrator

Vous activez une instance du Serveur de connexion pour l'authentification RSA SecurID ou l'authentification RADIUS en modifiant des paramètres du Serveur de connexion View dans View Administrator.

Prérequis

Installez et configurez le logiciel d'authentification à deux facteurs, tel que le logiciel RSA SecurID ou le logiciel RADIUS, sur un serveur de gestionnaires d'authentification.

- Pour l'authentification RSA SecurID, exportez le fichier `sdconf.rec` correspondant à l'instance du Serveur de connexion View à partir de RSA Authentication Manager. Reportez-vous à la documentation de RSA Authentication Manager.
- Pour l'authentification RADIUS, suivez la documentation de configuration du fournisseur. Notez le nom d'hôte ou l'adresse IP du serveur RADIUS, le numéro du port sur lequel il écoute l'authentification RADIUS (généralement 1812), le type d'authentification (PAP, CHAP, MS-CHAPv1 ou MS-CHAPv2) et la clé secrète partagée. Vous entrerez ces valeurs dans View Administrator. Vous pouvez entrer des valeurs pour un authentificateur RADIUS principal et secondaire.

Procédure

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

2 Dans l'onglet **Serveurs de connexion**, sélectionnez le serveur et cliquez sur **Modifier**.

3 Dans l'onglet **Authentification**, dans la liste déroulante **Authentification à deux facteurs** de la section Authentification avancée, sélectionnez **RSA SecureID** ou **RADIUS.**

4 Pour forcer les noms d'utilisateur RSA SecurID ou RADIUS à correspondre aux noms d'utilisateur d'Active Directory, sélectionnez **Appliquer la correspondance des noms d'utilisateur SecurID et Windows** ou **Appliquer la correspondance des noms d'utilisateur à deux 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 **Télécharger un fichier**, entrez l'emplacement du fichier `sdconf.rec` ou cliquez sur **Parcourir** pour rechercher le fichier.

6 Pour l'authentification RADIUS, renseignez le reste des champs :

a Sélectionnez **Utiliser les mêmes nom d'utilisateur et mot de passe pour l'authentification RADIUS et Windows** si l'authentification RADIUS initiale fait appel à l'authentification Windows qui déclenche une transmission hors bande d'un code de jeton et si ce code de jeton est ensuite utilisé dans le cadre d'un challenge RADIUS.

Si vous cochez cette case, les utilisateurs ne seront pas invités à fournir des informations d'identification Windows après l'authentification RADIUS si cette dernière utilise le nom d'utilisateur et le mode passe Windows. Les utilisateurs n'ont pas besoin d'entrer à nouveau le nom d'utilisateur et le mot de passe Windows après l'authentification RADIUS.

b Dans la liste déroulante **Authentificateur**, sélectionnez **Créer un nouvel authentificateur** et renseignez la page.

- Définissez **Port de gestion de compte** sur **0** sauf si vous souhaitez activer la gestion de compte RADIUS. Définissez ce port sur un numéro différent de zéro uniquement si votre serveur RADIUS prend en charge la collecte de données de gestion de compte. Si le serveur RADIUS ne prend pas en charge les messages de gestion de compte et si vous définissez ce port sur un numéro différent de zéro, les messages seront envoyés et ignorés, puis réessayés un certain nombre de fois, entraînant ainsi un retard d'authentification.

  Les données de gestion de compte peuvent être utilisées pour facturer les utilisateurs en fonction de la durée d'utilisation et des données échangées. Les données de gestion de compte peuvent également être utilisées à des fins statistiques ou pour la surveillance générale du réseau.

- Si vous spécifiez une chaîne de préfixe de domaine, celle-ci est placée au début du nom d'utilisateur lorsqu'il est envoyé au serveur RADIUS. Par exemple, si le nom d'utilisateur entré dans Horizon Client est **`jdoe`** et que le préfixe de domaine **`DOMAIN-A\`** est spécifié, le nom d'utilisateur **`DOMAIN-A\jdoe`** est envoyé au serveur RADIUS. De même, si vous utilisez le suffixe de domaine, ou postfix, la chaîne **`@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 prennent immédiatement effet.

Lorsque les utilisateurs ouvrent Horizon Client et s'authentifient sur le Serveur de connexion View, ils sont invités à fournir une authentification à deux facteurs. Pour l'authentification RADIUS, la boîte de dialogue d'ouverture de session affiche des invites qui contiennent l'étiquette du jeton que vous avez spécifié.

Les modifications apportées aux paramètres d'authentification RADIUS affectent les sessions d'applications et de postes de travail distants qui sont démarrées après la modification de la configuration. Les sessions en cours ne sont pas affectées par les modifications apportées aux paramètres d'authentification RADIUS.

Suivant

Si vous disposez d'un groupe répliqué d'instances du Serveur de connexion View et si vous souhaitez également configurer une authentification RADIUS sur celles-ci, vous pouvez réutiliser une configuration d'authentificateur RADIUS existante.

Résolution du refus d'accès RSA SecurID

L'accès est refusé lorsqu'Horizon Client se connecte avec l'authentification RSA SecurID.

Problème

Une connexion Horizon 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 **Configuration de View > Serveurs**.

2 Dans l'onglet **Serveurs de connexion**, sélectionnez le Serveur de connexion View et cliquez sur **Modifier**.

3 Sous l'onglet **Authentification**, sélectionnez **Effacer le code secret du nœud**.

4 Cliquez sur **OK** pour effacer le secret nœud.

5 Sur l'ordinateur qui exécute RSA Authentication Manager, sélectionnez **Démarrer > Programmes > RSA Security > Mode hôte RSA Authentication Manager**.

6 Sélectionnez **Hôte de l'agent > Modifier l'hôte de l'agent**.

7 Sélectionnez **Serveur de connexion View** dans la liste et décochez la case **Code secret du nœud créé**.

Code secret du nœud créé est sélectionné par défaut chaque fois que vous le modifiez.

8 Cliquez sur **OK**.

Résolution du refus d'accès RADIUS

L'accès est refusé lorsqu'Horizon Client se connecte avec l'authentification à deux facteurs RADIUS.

Problème

Une connexion Horizon Client à l'aide de l'authentification à deux facteurs RADIUS affiche `Access Denied`.

Cause

RADIUS ne reçoit pas de réponse du serveur RADIUS, ce qui provoque l'expiration du délai d'attente de View.

Solution

Les erreurs de configuration courantes qui conduisent le plus souvent à cette situation sont les suivantes :

- Le serveur RADIUS n'a pas été configuré pour accepter l'instance du Serveur de connexion View en tant que client RADIUS. Chaque instance du Serveur de connexion View utilisant RADIUS doit être configurée en tant que client sur le serveur RADIUS. Reportez-vous à la documentation concernant votre produit d'authentification à deux facteurs RADIUS.
- La valeur de secret partagé de l'instance du Serveur de connexion View et celle du serveur RADIUS ne correspondent pas.

Utilisation de l'authentification SAML

Le langage SAML (Security Assertion Markup Language) est une norme XML utilisée pour décrire et échanger des informations d'authentification et d'autorisation entre différents domaines de sécurité. SAML transmet des informations sur les utilisateurs entre les fournisseurs d'identité et les fournisseurs de services dans des documents XML nommés assertions SAML.

Vous pouvez utiliser l'authentification SAML pour intégrer View à VMware Workspace Portal, VMware Identity Manager ou une passerelle ou un équilibrage de charge tiers. Lorsque la fonctionnalité SSO est activée, les utilisateurs qui ouvrent une session sur VMware Identity Manager ou un périphérique tiers peuvent lancer des applications et des postes de travail distants sans passer par une deuxième procédure de connexion. Vous pouvez également utiliser l'authentification SAML pour implémenter l'authentification par carte à puce sur VMware Access Point ou sur des périphériques tiers.

Pour déléguer la responsabilité de l'authentification à Workspace Portal, VMware Identity Manager ou un périphérique tiers, vous devez créer un authentificateur SAML dans View. Un authentificateur SAML contient l'approbation et l'échange de métadonnées entre View et Workspace Portal, VMware Identity Manager ou le périphérique tiers. Vous associez un authentificateur SAML à une instance du Serveur de connexion View.

Utilisation de l'authentification SAML pour l'intégration de VMware Identity Manager

L'intégration entre View et VMware Identity Manager (dont le nom était précédemment Workspace Portal) fait appel à la norme SAML 2.0 pour établir une approbation mutuelle, qui est essentielle pour la fonctionnalité d'authentification unique. Lorsque l'authentification unique est activée, les utilisateurs qui se connectent à VMware Identity Manager ou Workspace Portal avec des informations d'identification Active Directory peuvent lancer des applications et des postes de travail distants sans passer par une deuxième procédure de connexion.

Lorsque VMware Identity Manager et View sont intégrés, VMware Identity Manager génère un artefact SAML unique dès qu'un utilisateur se connecte à VMware Identity Manager et clique sur une icône de poste de travail ou d'application. VMware Identity Manager utilise cet artefact SAML pour créer un URI (Universal Resource Identifier). L'URI contient des informations sur l'instance du Serveur de connexion View sur laquelle réside le pool de postes de travail ou d'applications, sur le poste de travail ou l'application à lancer et sur l'artefact SAML.

VMware Identity Manager envoie l'artefact SAML à Horizon Client, qui à son tour envoie l'artefact à l'instance du Serveur de connexion View. L'instance du Serveur de connexion View utilise l'artefact SAML pour récupérer l'assertion SAML de VMware Identity Manager.

Dès qu'une instance du Serveur de connexion View reçoit une assertion SAML, elle valide celle-ci, déchiffre le mot de passe de l'utilisateur et utilise le mot de passe déchiffré pour lancer le poste de travail ou l'application.

L'installation de l'intégration de VMware Identity Manager et de View implique la configuration de VMware Identity Manager avec les informations de View et la configuration de View afin de déléguer la responsabilité de l'authentification à VMware Identity Manager.

Pour déléguer la responsabilité de l'authentification à VMware Identity Manager, vous devez créer un authentificateur SAML dans View. Un authentificateur SAML assure l'échange d'approbations et de métadonnées entre View et VMware Identity Manager. Vous associez un authentificateur SAML à une instance du Serveur de connexion View.

Remarque Si vous prévoyez de fournir un accès à vos applications et postes de travail via VMware Identity Manager, assurez-vous de créer les pools d'applications et de postes de travail en tant qu'utilisateur disposant du rôle Administrateurs sur le groupe d'accès racine dans View Administrator. Si vous attribuez à l'utilisateur le rôle Administrateurs sur un groupe d'accès autre que le groupe d'accès racine, VMware Identity Manager ne reconnaîtra pas l'authentificateur SAML que vous configurez dans View et vous ne pourrez pas configurer le pool dans VMware Identity Manager.

Configurer un authentificateur SAML dans View Administrator

Pour lancer des applications et des postes de travail distants depuis VMware Identity Manager ou pour vous connecter à des applications et des postes de travail distants via une passerelle ou un équilibrage de charge tiers, vous devez créer un authentificateur SAML dans View Administrator. Un authentificateur SAML contient l'approbation et l'échange de métadonnées entre View et le périphérique auquel se connectent les clients.

Vous associez un authentificateur SAML à une instance du Serveur de connexion View. Si votre déploiement inclut plusieurs instances du Serveur de connexion View, vous devez associer l'authentificateur SAML à chaque instance.

Vous pouvez autoriser la mise en service d'un authentificateur statique et de plusieurs authentificateurs dynamiques à la fois. Vous pouvez configurer des authentificateurs vIDM (Dynamique) et Access Point (Statique) et les conserver dans un état actif. Vous pouvez établir des connexions via l'un de ces authentificateurs.

Vous pouvez configurer plusieurs authentificateurs SAML sur un Serveur de connexion View et tous les authentificateurs peuvent être actifs simultanément. Toutefois, l'ID d'entité de chacun de ces authentificateurs SAML configurés sur le Serveur de connexion View doit être différent.

L'état de l'authentificateur SAML dans le tableau de bord est toujours vert, car il s'agit de métadonnées prédéfinies qui sont statiques par nature. Le basculement entre le rouge et le vert ne s'applique que pour les authentificateurs dynamiques.

Pour plus d'informations sur la configuration d'un authentificateur SAML pour les dispositifs Access Point de VMware, consultez le document *Déploiement et configuration d'Access Point*.

Prérequis

- Vérifiez qu'Workspace Portal, VMware Identity Manager ou une passerelle ou un équilibrage de charge tiers est installé et configuré. Consultez la documentation d'installation de ce produit.
- Vérifiez que le certificat racine de l'autorité de certification de signature pour le certificat du serveur SAML est installé sur l'hôte du serveur de connexion. VMware recommande de ne pas configurer d'authentificateurs SAML pour utiliser des certificats auto-signés. Pour plus d'informations sur l'authentification des certificats, reportez-vous au document *Installation de View*.
- Notez le nom de domaine complet ou l'adresse IP du serveur Workspace Portal, du serveur VMware Identity Manager ou de l'équilibrage de charge externe.
- (Facultatif) Si vous utilisez Workspace Portal ou VMware Identity Manager, notez l'URL de l'interface Web du connecteur.
- Si vous créez un authentificateur pour Access Point ou un dispositif tiers qui exige que vous génériez des métadonnées SAML et que vous créiez un authentificateur statique, exécutez la procédure sur le périphérique pour générer les métadonnées SAML, puis copiez les métadonnées.

Procédure

1 Dans View Administrator, sélectionnez **Configuration > Serveurs**.

2 Dans l'onglet **Serveurs de connexion**, sélectionnez une instance du serveur à associer à l'authentificateur SAML et cliquez sur **Modifier**.

3 Dans l'onglet **Authentification**, sélectionnez un paramètre dans le menu déroulant**Délégation de l'authentification à VMware Horizon (authentificateur SAML 2.0)** pour activer ou désactiver l'authentificateur SAML.

Option	Description
Désactivé	L'authentification SAML est désactivée. Vous ne pouvez lancer des applications et des postes de travail distants qu'à partir d'Horizon Client.
Autorisé	L'authentification SAML est activée. Vous pouvez lancer des applications et des postes de travail distants depuis Horizon Client et VMware Identity Manager ou le périphérique tiers.
Requis	L'authentification SAML est activée. Vous pouvez lancer des applications et des postes de travail distants uniquement depuis VMware Identity Manager ou le périphérique tiers. Vous ne pouvez pas lancer manuellement des postes de travail ou des applications à partir d'Horizon Client.

Vous pouvez configurer chaque instance du Serveur de connexion View dans votre déploiement pour disposer de paramètres d'authentification SAML différents, adaptés à vos exigences.

4 Cliquez sur **Gérer des authentificateurs SAML**, puis sur **Ajouter**.

5 Configurez l'authentificateur SAML dans la boîte de dialogue Ajouter un authentificateur SAML 2.0.

Option	Description
Type	Pour Access Point ou un périphérique tiers, sélectionnez **Statique**. Pour VMware Identity Manager sélectionnez **Dynamique**. Pour les authentificateurs dynamiques, vous pouvez spécifiez une URL de métadonnées et une URL d'administration. Pour les authentificateurs statiques, vous devez d'abord générer les métadonnées sur Access Point ou sur un périphérique tiers, copier les métadonnées, puis les coller dans la zone de texte **Métadonnées SAML**.
Étiquette	Nom unique qui identifie l'authentificateur SAML.
Description	Brève description de l'authentificateur SAML. Cette valeur est facultative.
URL de métadonnées	(Pour les authentificateurs dynamiques) URL pour récupérer toutes les informations requises pour échanger des informations SAML entre le fournisseur d'identité SAML et l'instance du Serveur de connexion View. Dans l'URL `https://<NOM DE VOTRE SERVEUR HORIZON>/SAAS/API/1.0/GET/metadata/idp.xml`, cliquez sur **<NOM DE VOTRE SERVEUR HORIZON>** et remplacez-le par le FQDN ou l'adresse IP du serveur VMware Identity Manager ou de l'équilibrage de charge externe (périphérique tiers).
URL d'administration	(Pour les authentificateurs dynamiques) URL pour accéder à la console d'administration du fournisseur d'identité SAML. Pour VMware Identity Manager, cette URL doit pointer vers l'interface Web d'VMware Identity Manager Connector. Cette valeur est facultative.
Métadonnées SAML	(Pour les authentificateurs statiques) Texte des métadonnées que vous avez générées et copiées depuis Access Point ou depuis un périphérique tiers.
Activé pour le Serveur de connexion	Cochez cette case pour activer l'authentificateur. Vous pouvez activer plusieurs authentificateurs. Seuls les authentificateurs activés sont affichés dans la liste.

6 Cliquez sur **OK** pour enregistrer la configuration de l'authentificateur SAML.

Si vous avez fourni des informations valides, vous devez accepter le certificat auto-signé (non recommandé) ou utiliser un certificat approuvé pour View et VMware Identity Manager ou le périphérique tiers.

La boîte de dialogue Gérer des authentificateurs SAML affiche l'authentificateur récemment créé.

7 Dans la section Intégrité du système du tableau de bord de View Administrator, sélectionnez **Autres composants > Authentificateurs SAML 2.0**, sélectionnez l'authentificateur SAML que vous avez ajouté, puis vérifiez les détails.

Si la configuration aboutit, la santé de l'authentificateur est représentée par la couleur verte. La santé de l'authentificateur peut s'afficher en rouge si le certificat n'est pas approuvé, si VMware Identity Manager n'est pas disponible ou si l'URL des métadonnées n'est pas valide. Si le certificat n'est pas approuvé, vous pourrez peut-être cliquer sur **Vérifier** pour valider et accepter le certificat.

Suivant

Étendez la période d'expiration des métadonnées du Serveur de connexion View pour que les sessions à distance ne se terminent pas après seulement 24 heures. Reportez-vous à la section « Modifier la période d'expiration des métadonnées du fournisseur de services sur le Serveur de connexion View », page 75.

Modifier la période d'expiration des métadonnées du fournisseur de services sur le Serveur de connexion View

Si vous ne modifiez pas la période d'expiration, le Serveur de connexion View cessera d'accepter les assertions SAML de l'authentificateur SAML, tel qu'Access Point ou un fournisseur d'identité tiers, après 24 heures, et l'échange de métadonnées doit être répété.

Suivez cette procédure pour indiquer le délai en jours après lequel le Serveur de connexion View arrête d'accepter les assertions SAML du fournisseur d'identité. Cette valeur est utilisée à la fin de la période d'expiration actuelle. Par exemple, si la période d'expiration actuelle est d'un jour et que vous indiquez 90 jours, lorsque le délai d'un jour est écoulé, le Serveur de connexion View génère des métadonnées avec une période d'expiration de 90 jours.

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 du Serveur de connexion View.

2 Dans l'arborescence de la console, sélectionnez **Se connecter à**.

3 Dans la zone de texte **Sélectionnez ou entrez un nom unique ou un contexte d'attribution de noms**, tapez le nom unique **`DC=vdi, DC=vmware, DC=int`**.

4 Dans le volet Ordinateur, sélectionnez ou tapez **`localhost:389`** ou le nom de domaine complet du Serveur de connexion View, suivi du port 389.

   Par exemple : **`localhost:389`** ou **`mycomputer.example.com:389`**

5 Développez l'arborescence de l'Éditeur ADSI, développez **OU=Properties**, sélectionnez **OU=Global** et double-cliquez sur **CN=Common** dans le volet de droite.

6 Dans la boîte de dialogue Propriétés, modifiez l'attribut **pae-NameValuePair** pour ajouter les valeurs suivantes

   ```
   cs-samlencryptionkeyvaliditydays=number-of-days
   cs-samlsigningkeyvaliditydays=number-of-days
   ```

   Dans cet exemple, *number-of-days* est le nombre de jours pouvant s'écouler avant qu'un Serveur de connexion View distant cesse d'accepter des assertions SAML. Après cette période de temps, le processus d'échange des métadonnées SAML doit être répété.

Générer des métadonnées SAML pour que le Serveur de connexion View puisse être utilisé comme fournisseur de services

Après avoir créé et activé un authentificateur SAML pour le fournisseur d'identité que vous voulez utiliser, vous devrez peut-être générer des métadonnées du Serveur de connexion View. Vous utilisez ces métadonnées pour créer un fournisseur de services sur le dispositif Access Point ou un équilibrage de charge tiers qui est le fournisseur d'identité.

Prérequis

Vérifiez que vous avez créé un authentificateur SAML pour le fournisseur d'identité : Access Point ou une passerelle ou un équilibrage de charge tiers. Dans la section Intégrité du système du tableau de bord de View Administrator, vous pouvez sélectionner **Autres composants > Authentificateurs SAML 2.0**, sélectionner l'authentificateur SAML que vous avez ajouté, puis vérifier les détails.

Procédure

1 Ouvrez un nouvel onglet dans le navigateur et entrez l'URL pour obtenir les métadonnées SAML du Serveur de connexion View.

`https://connection-server.example.com/SAML/metadata/sp.xml`

Dans cet exemple, *connection-server.example.com* est le nom de domaine complet de l'hôte du Serveur de connexion View.

Cette page affiche les métadonnées SAML du Serveur de connexion View.

2 Utilisez une commande **Enregistrer sous** pour enregistrer la page Web en tant que fichier XML.

Par exemple, vous pouvez enregistrer la page sous forme d'un fichier avec le nom `connection-server-metadata.xml`. Le contenu de ce fichier commence par le texte suivant :

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" ...
```

Suivant

Utilisez la procédure appropriée sur le fournisseur d'identité pour copier les métadonnées SAML du Serveur de connexion View. Consultez la documentation d'Access Point ou d'une passerelle ou d'un équilibrage de charge tiers.

Considérations sur le temps de réponse pour plusieurs authentificateurs SAML dynamiques

Si vous configurez l'authentification SAML 2.0 pour qu'elle soit facultative ou obligatoire sur une instance du Serveur de connexion View et que vous associez plusieurs authentificateurs SAML dynamiques à l'instance du Serveur de connexion View, si des authentificateurs SAML dynamiques deviennent inaccessibles, le temps de réponse pour lancer des postes de travail distants à partir des autres authentificateurs SAML dynamiques augmente.

Vous pouvez réduire le temps de réponse pour le lancement des postes de travail distants sur les autres authentificateurs SAML dynamiques en utilisant View Administrator pour désactiver les authentificateurs SAML dynamiques. Pour plus d'informations sur la désactivation d'un authentificateur SAML, reportez-vous à la section « Configurer un authentificateur SAML dans View Administrator », page 72.

Configurer l'authentification biométrique

Vous pouvez configurer l'authentification biométrique en modifiant l'attribut `pae-ClientConfig` dans la base de données LDAP.

Prérequis

Pour plus d'informations sur l'utilisation de l'utilitaire ADSI Edit sur votre serveur Windows, consultez le site Web Microsoft TechNet.

Procédure

1 Démarrez l'utilitaire ADSI Edit sur l'hôte du Serveur de connexion View.

2 Dans la boîte de dialogue Paramètres de connexion, sélectionnez **DC=vdi,DC=vmware,DC=int** ou connectez-vous à cet objet.

3 Dans le volet Ordinateur, sélectionnez ou tapez **`localhost:389`** ou le nom de domaine complet du 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**, modifiez l'attribut **pae-ClientConfig** et ajoutez la valeur **BioMetricsTimeout=<integer>**.

Les valeurs `BioMetricsTimeout` suivantes sont valides :

Valeur BioMetricsTimeout	Description
0	L'authentification biométrique n'est pas prise en charge. Il s'agit du réglage par défaut.
-1	L'authentification biométrique est prise en charge sans limite de temps.
N'importe quel entier positif	L'authentification biométrique est prise en charge et peut être utilisée pendant le nombre de minutes spécifié.

Le nouveau paramètre prend effet immédiatement. Vous n'avez pas à redémarrer le service Serveur de connexion View ou le périphérique client.

Authentification des utilisateurs sans demander les informations d'identification

5

Lorsque les utilisateurs sont connectés à un périphérique client ou à VMware Identity Manager, ils peuvent se connecter à une application ou un poste de travail publié sans être invités à fournir leurs informations d'identification Active Directory.

Les administrateurs peuvent choisir d'effectuer la configuration en fonction des exigences de l'utilisateur.

- Fournissez aux utilisateurs un accès non authentifié à des applications publiées. Les administrateurs peuvent configurer l'installation de sorte que les utilisateurs n'aient pas besoin de se connecter à Horizon Client avec des informations d'identification Active Directory (AD).
- Utilisez Se connecter en tant qu'utilisateur actuel pour les clients Windows. Pour les clients Windows, les administrateurs peuvent configurer l'installation afin que les utilisateurs n'aient pas à fournir des informations d'identification supplémentaires pour se connecter à un serveur Horizon Server après s'être connectés à un client Windows avec des informations d'identification AD.
- Enregistrez les informations d'identification dans les clients Horizon Client pour Mac et mobiles. Pour les clients mobiles et les clients Mac, les administrateurs peuvent configurer Horizon Server pour qu'il enregistre les informations d'identification. Avec cette fonctionnalité, les utilisateurs n'ont pas à mémoriser leurs informations d'identification AD pour l'authentification unique (Single Sign-On) une fois qu'ils les ont fournies à un client mobile ou à un client Mac.
- Configurez l'authentification unique réelle pour VMware Identity Manager. Pour VMware Identity Manager, les administrateurs peuvent configurer l'authentification unique réelle afin que les utilisateurs qui s'authentifient avec une méthode autre que les informations d'identification AD puissent ensuite se connecter à une application ou un poste de travail distant sans être invités à fournir des informations d'identification AD.

Ce chapitre aborde les rubriques suivantes :

Fourniture d'un accès non authentifié pour des applications publiées

Les administrateurs peuvent effectuer la configuration pour que les utilisateurs non authentifiés puissent accéder à leurs applications publiées depuis une instance d'Horizon Client sans informations d'identification AD. Envisagez de configurer l'accès non authentifié si vos utilisateurs doivent accéder à une application déportée disposant de sa propre gestion de la sécurité et des utilisateurs.

Lorsqu'un utilisateur démarre une application publiée configurée pour l'accès non authentifié, l'hôte RDS crée une session d'utilisateur local à la demande et alloue la session à l'utilisateur.

Cette fonctionnalité requiert l'environnement Horizon 7 version 7.1 et Horizon Client version 4.4.

Workflow pour configurer des utilisateurs non authentifiés

1. Créez des utilisateurs pour l'accès non authentifié. Reportez-vous à la section « Créer des utilisateurs pour l'accès non authentifié », page 81.
2. Activez l'accès non authentifié pour des utilisateurs et définissez un utilisateur non authentifié par défaut. Reportez-vous à la section « Activer l'accès non authentifié pour des utilisateurs », page 82.
3. Autorisez les utilisateurs d'accès non authentifié à accéder à des applications publiées. Reportez-vous à la section « Autoriser les utilisateurs d'accès non authentifié à accéder à des applications publiées », page 82.
4. Activez l'accès non authentifié à partir d'Horizon Client. Reportez-vous à la section « Accès non authentifié depuis Horizon Client », page 84.

Règles et recommandations pour configurer des utilisateurs non authentifiés

- L'authentification à deux facteurs, telle que RSA et RADIUS, et l'authentification par carte à puce ne sont pas prises en charge pour l'accès non authentifié.
- L'authentification par carte à puce et l'accès non authentifié s'excluent mutuellement. Lorsque l'authentification par carte à puce est définie sur **Obligatoire** dans le Serveur de connexion, l'accès non authentifié est désactivé même s'il était activé précédemment.
- VMware Identity Manager et VMware App Volumes ne sont pas pris en charge pour l'accès non authentifié.
- La connexion avec accès non authentifié à partir du client HTML Access n'est pas prise en charge.
- Les protocoles d'affichage PCoIP et VMware Blast sont pris en charge pour cette fonctionnalité.
- La fonctionnalité d'accès non authentifié ne vérifie pas les informations sur la licence des hôtes RDS. L'administrateur doit configurer et utiliser des licences de périphérique.
- La fonctionnalité d'accès non authentifié ne conserve pas les données spécifiques de l'utilisateur. L'utilisateur peut vérifier les exigences de stockage des données de l'application.
- Vous ne pouvez pas vous reconnecter à des sessions d'application non authentifiées. Lorsqu'un utilisateur se déconnecte du client, l'hôte RDS ferme la session d'utilisateur local automatiquement.
- L'accès non authentifié n'est pris en charge que pour les applications publiées.
- L'accès non authentifié n'est pas pris en charge avec un serveur de sécurité ou un dispositif Access Point.
- Les préférences utilisateur ne sont pas conservées pour les utilisateurs non authentifiés.
- Les postes de travail virtuels ne sont pas pris en charge pour les utilisateurs non authentifiés.

- Horizon Administrator affiche un état rouge pour le Serveur de connexion, si ce dernier est configuré avec un certificat signé par une autorité de certification et activé pour l'accès non authentifié, mais qu'aucun utilisateur non authentifié par défaut n'est configuré.
- La fonctionnalité d'accès non authentifié n'est pas opérationnelle si la stratégie de groupe `AllowSingleSignon` pour Horizon Agent installé sur un hôte RDS est désactivée. Les administrateurs peuvent également contrôler s'il faut désactiver ou activer l'accès non authentifié avec le paramètre de stratégie de groupe `UnAuthenticatedAccessEnabled` d'Horizon Agent. Les paramètres de stratégie de groupe d'Horizon Agent sont inclus dans le fichier de modèle d'administration ADMX (`vdm_agent.admx`) ou ADM (`vdm_agent.adm`). Vous devez redémarrer l'hôte RDS pour que cette stratégie prenne effet.

Créer des utilisateurs pour l'accès non authentifié

Les administrateurs peuvent créer des utilisateurs pour l'accès non authentifié à des applications publiées. Lorsqu'un administrateur configure un utilisateur pour l'accès non authentifié, l'utilisateur peut se connecter à l'instance du Serveur de connexion à partir d'Horizon Client uniquement avec l'accès non authentifié.

Prérequis

- Vérifiez que l'utilisateur Active Directory (AD) pour lequel vous voulez configurer l'accès non authentifié dispose d'un UPN valide. Seul un utilisateur AD peut être configuré en tant qu'utilisateur ne disposant pas d'un accès non authentifié.

Remarque Les administrateurs ne peuvent créer qu'un seul utilisateur pour chaque compte AD. Les administrateurs ne peuvent pas créer des groupes d'utilisateurs non authentifiés. Si vous créez un utilisateur d'accès non authentifié et qu'il existe une session cliente pour cet utilisateur AD, vous devez redémarrer la session cliente pour que les modifications prennent effet.

Procédure

1. Dans Horizon Administrator, sélectionnez **Utilisateurs et groupes**.
2. Dans l'onglet **Accès non authentifié**, cliquez sur **Ajouter**.
3. Dans l'assistant Ajouter un utilisateur non authentifié, sélectionnez un ou plusieurs critères de recherche et cliquez sur **Rechercher** pour trouver les utilisateurs correspondants à vos critères.

   L'utilisateur doit disposer d'un UPN valide.
4. Sélectionnez un utilisateur et cliquez sur **Suivant**.

   Répétez cette étape pour ajouter plusieurs utilisateurs.
5. (Facultatif) Entrez l'alias d'utilisateur.

   L'alias d'utilisateur par défaut est le nom d'utilisateur qui a été configuré pour le compte AD. Les utilisateurs finaux peuvent utiliser l'alias d'utilisateur pour se connecter à l'instance du Serveur de connexion à partir d'Horizon Client.
6. (Facultatif) Examinez les détails utilisateur et ajoutez des commentaires.
7. Cliquez sur **Terminer**.

Le Serveur de connexion crée l'utilisateur d'accès non authentifié et affiche ses détails, notamment l'alias d'utilisateur, le nom d'utilisateur, le prénom et le nom de famille, le nombre d'espaces source, de droits d'application et de sessions. Vous pouvez cliquer sur le nombre dans la colonne Espaces source pour afficher des informations sur l'espace.

Suivant

Activez l'accès non authentifié pour les utilisateurs dans le Serveur de connexion. Reportez-vous à la section « Activer l'accès non authentifié pour des utilisateurs », page 82.

Activer l'accès non authentifié pour des utilisateurs

Une fois que vous avez créé des utilisateurs pour l'accès non authentifié, vous devez activer l'accès non authentifié dans le Serveur de connexion pour autoriser les utilisateurs à se connecter et à accéder à des applications publiées.

Procédure

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

2 Cliquez sur l'onglet **Serveurs de connexion**.

3 Sélectionnez l'instance du Serveur de connexion et cliquez sur **Modifier**.

4 Cliquez sur l'onglet **Authentification**.

5 Remplacez **Accès non authentifié** par **Activé**.

6 Dans le menu déroulant **Utilisateur d'accès non authentifié par défaut**, sélectionnez un utilisateur comme utilisateur par défaut.

L'utilisateur par défaut doit être présent dans l'espace local d'un environnement Architecture Cloud Pod. Si vous sélectionnez un utilisateur par défaut d'un espace différent, le Serveur de connexion crée l'utilisateur sur l'espace local avant d'en faire l'utilisateur par défaut.

7 (Facultatif) Entrez le délai d'expiration de la session par défaut pour l'utilisateur.

Le délai d'expiration de la session par défaut est de 10 minutes après l'inactivité.

8 Cliquez sur **OK**.

Suivant

Autorisez les utilisateurs d'accès non authentifié à accéder à des applications publiées. Reportez-vous à la section « Autoriser les utilisateurs d'accès non authentifié à accéder à des applications publiées », page 82.

Autoriser les utilisateurs d'accès non authentifié à accéder à des applications publiées

Une fois que vous avez créé un utilisateur d'accès non authentifié, vous devez autoriser l'utilisateur à accéder à des applications publiées.

Prérequis

- Créez une batterie de serveurs basée sur un groupe d'hôtes RDS. Reportez-vous à la section « Création de batteries de serveurs » dans le document *Configuration d'applications et de postes de travail publiés dans Horizon 7*.
- Créez un pool d'applications pour des applications publiées exécutées sur une batterie de serveurs d'hôtes RDS. Reportez-vous à la section « Création de pools d'applications » dans le document *Configuration d'applications et de postes de travail publiés dans Horizon 7*.

Procédure

1 Dans Horizon Administrator, sélectionnez **Catalogue > Pools d'applications** et cliquez sur le nom du pool d'applications.

2 Sélectionnez **Ajouter un droit** dans le menu déroulant **Autorisations**.

3 Cliquez sur **Ajouter**, sélectionnez un ou plusieurs critères de recherche, cliquez sur **Rechercher** et cochez la case **Utilisateurs non authentifiés** pour trouver les utilisateurs d'accès non authentifié correspondants à vos critères.

4 Sélectionnez les utilisateurs que vous voulez autoriser à accéder aux applications dans le pool et cliquez sur **OK**.

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

Une icône d'accès non authentifié s'affiche en regard de l'utilisateur d'accès non authentifié une fois que le processus d'autorisation est terminé.

Suivant

Utilisez un utilisateur d'accès non authentifié pour vous connecter à Horizon Client. Reportez-vous à la section « Accès non authentifié depuis Horizon Client », page 84.

Rechercher des sessions avec un accès non authentifié

Utilisez Horizon Administrator pour répertorier ou rechercher les sessions d'application auxquelles des utilisateurs d'accès non authentifié sont connectés. L'icône d'utilisateur d'accès non authentifié s'affiche en regard de ces sessions.

Procédure

1 Dans Horizon Administrator, sélectionnez **Contrôle > Sessions**.

2 Cliquez sur **Applications** pour rechercher des sessions d'application.

3 Sélectionnez les critères de recherche et commencez la recherche.

Les résultats de la recherche incluent l'utilisateur, le type de session (poste de travail ou application), la machine, le pool ou la batterie de serveurs, le nom DNS, l'ID de client et la passerelle de sécurité. La date de début de la session, sa durée, son état et la dernière session s'affichent également dans les résultats de la recherche.

Supprimer un utilisateur d'accès non authentifié

Lorsque vous supprimez un utilisateur d'accès non authentifié, vous devez également supprimer les droits de pool d'applications pour l'utilisateur. Vous ne pouvez pas supprimer un utilisateur d'accès non authentifié qui est l'utilisateur par défaut.

Remarque Si vous supprimez un utilisateur d'accès non authentifié et qu'il existe une session cliente pour cet utilisateur AD, vous devez redémarrer la session cliente pour que les modifications prennent effet.

Procédure

1 Dans Horizon Administrator, sélectionnez **Utilisateurs et groupes**.

2 Dans l'onglet **Accès non authentifié**, cliquez sur **Supprimer**.

3 Cliquez sur **OK**.

Suivant

Supprimez des droits d'application pour l'utilisateur. Reportez-vous à la section « Supprimer des droits d'un pool de postes de travail ou d'applications » dans le document *Configuration d'applications et de postes de travail publiés dans Horizon 7*.

Accès non authentifié depuis Horizon Client

Connectez-vous à Horizon Client avec un accès non authentifié et démarrez l'application publiée.

Pour garantir une meilleure sécurité, l'utilisateur sans accès authentifié dispose d'un alias utilisateur que vous pouvez utiliser pour vous connecter à Horizon Client. Lorsque vous sélectionnez un alias utilisateur, vous n'avez pas besoin de fournir les informations d'identification AD ou l'UPN de l'utilisateur. Une fois connecté à Horizon Client, vous pouvez cliquer sur vos applications publiées pour les démarrer. Pour plus d'informations sur l'installation et la configuration de clients Horizon Client, consultez la documentation d'Horizon Client sur la page Web de la documentation de VMware Horizon Clients.

Prérequis

- Vérifiez que le Serveur de connexion Horizon 7 version 7.1 est configuré pour l'accès non authentifié.
- Vérifiez que les utilisateurs sans accès authentifié sont créés dans Horizon Administrator. Si l'utilisateur non authentifié par défaut est le seul utilisateur sans accès authentifié, Horizon Client se connecte à l'instance du Serveur de connexion avec l'utilisateur par défaut.

Procédure

1. Démarrez Horizon Client.
2. Dans Horizon Client, sélectionnez **Se connecter de manière anonyme avec un accès non authentifié**.
3. Connectez-vous à l'instance du Serveur de connexion.
4. Sélectionnez un alias utilisateur dans le menu déroulant et cliquez sur **Connexion**.

   L'utilisateur par défaut présente le suffixe « default ».
5. Double-cliquez sur une application publiée pour la démarrer.

Utilisation de la fonctionnalité Se connecter en tant qu'utilisateur actuel, disponible avec Horizon Client pour Windows

Avec Horizon 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 du Serveur de connexion View et sur le poste de travail distant. 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 d'Horizon 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 des paramètres de stratégie de groupe Horizon Client pour contrôler la disponibilité de la case à cocher **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 lorsqu'il coche la case **Se connecter en tant qu'utilisateur actuel** dans Horizon Client.

La fonction Se connecter en tant qu'utilisateur actuel a les limites 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 le Serveur de connexion View.
- 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 droits d'usage par défaut **Accéder à cet ordinateur à partir du réseau** sont modifiées sur le système client, elles doivent être modifiées 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.

Enregistrement des informations d'identification dans Horizon Client pour Mac et mobiles

Les administrateurs peuvent configurer le Serveur de connexion View pour permettre à Horizon Client pour Mac et mobiles de mémoriser le nom d'utilisateur, le mot de passe et les informations de domaine d'un utilisateur.

Dans Horizon Client pour appareils mobiles, cette fonctionnalité entraîne l'apparition de la case **Enregistrer le mot de passe** dans les boîtes de dialogue de connexion. Dans Horizon Client pour Mac, cette fonctionnalité entraîne l'apparition de la case **Mémoriser ce mot de passe** dans la boîte de dialogue de connexion.

Si les utilisateurs choisissent d'enregistrer leurs informations d'identification, celles-ci sont ajoutées aux champs de connexion dans Horizon Client lors des connexions suivantes.

Pour activer cette fonctionnalité, vous devez définir une valeur dans View LDAP pour indiquer la durée de l'enregistrement des informations d'identification dans le client. Dans Horizon Client pour Mac, cette fonctionnalité est prise en charge uniquement dans la version 4.1 ou ultérieure.

Remarque Sur les clients Horizon basés sur Windows, la fonctionnalité de connexion en tant qu'utilisateur actuel évite d'obliger les utilisateurs à fournir des informations d'identification à plusieurs reprises.

Configurer une limite du délai d'expiration pour enregistrer les informations d'identification d' Horizon Client

Vous configurez une limite du délai d'expiration qui indique au bout de combien temps enregistrer les informations d'identification d'Horizon Client sur les périphériques mobiles et les systèmes clients Mac 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 du Serveur de connexion View, la modification est propagée à toutes les instances du 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 du Serveur de connexion View.

2 Dans la boîte de dialogue Paramètres de connexion, sélectionnez **DC=vdi,DC=vmware,DC=int** ou connectez-vous à cet objet.

3 Dans le volet Ordinateur, sélectionnez ou tapez **`localhost:389`** ou le nom de domaine complet du 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**, modifiez la valeur d'attribut **clientCredentialCacheTimeout**.

   Lorsque `clientCredentialCacheTimeout` n'est pas défini ou est défini sur **`0`**, la fonctionnalité est désactivée. Pour activer cette fonctionnalité, vous pouvez définir le nombre de minutes de conservation des informations d'identification, ou définir une valeur de **-1**, ce qui signifie qu'il n'y a pas de délai d'expiration.

Dans le Serveur de connexion View, le nouveau paramètre s'applique immédiatement. Vous n'avez pas à redémarrer le service Serveur de connexion View ou l'ordinateur client.

Configuration de l'authentification unique réelle

Avec la fonctionnalité d'authentification unique réelle, une fois que les utilisateurs sont connectés à VMware Identity Manager à l'aide de l'authentification par carte à puce, RSA SecurID ou RADIUS, ils n'ont pas à entrer également leurs informations d'identification Active Directory pour utiliser une application ou un poste de travail distant.

Si un utilisateur s'authentifie avec des informations d'identification Active Directory, la fonctionnalité d'authentification unique réelle n'est pas nécessaire, mais vous pouvez la configurer pour qu'elle soit utilisée même dans ce cas, afin que les informations d'identification AD que l'utilisateur fournit soient ignorées et que l'authentification unique réelle soit utilisée.

Lorsqu'ils se connectent à un poste de travail virtuel ou à une application distante, les utilisateurs peuvent choisir d'utiliser Horizon Client ou HTML Access natif.

Cette fonction présente les limites suivantes :

- Cette fonctionnalité n'est pas opérationnelle pour les postes de travail virtuels qui sont fournis via l'utilisation du plug-in View Agent Direct Connection.
- Cette fonctionnalité n'est prise en charge que dans les environnements IPv4.

Voici une liste des tâches que vous devez effectuer pour configurer votre environnement pour l'authentification unique réelle :

1 « Déterminer une architecture pour l'authentification unique réelle », page 87

2 « Configurer une autorité de certification d'entreprise », page 89

3 « Créer des modèles de certificat utilisés avec l'authentification unique réelle », page 91

4 « Installer et configurer un serveur d'inscription », page 93

5 « Exporter le certificat Client de service d'inscription », page 95

6 « Configurer l'authentification SAML pour l'utiliser avec l'authentification unique réelle », page 97

7 « Configurer le Serveur de connexion View pour l'authentification unique réelle », page 99

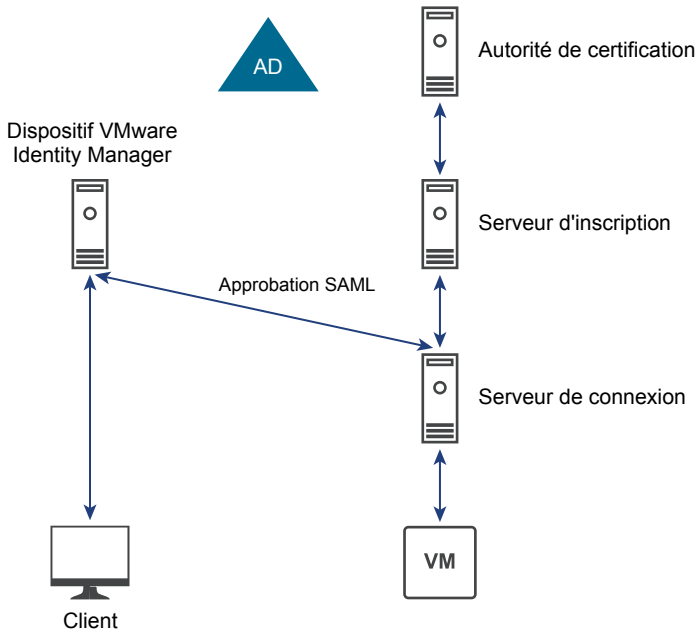
Déterminer une architecture pour l'authentification unique réelle

Pour utiliser l'authentification unique réelle, vous devez disposer d'une autorité de certification, ou en ajouter une, et créer un serveur d'inscription. Ces deux serveurs communiquent pour créer le certificat virtuel Horizon de courte durée qui permet d'effectuer une ouverture de session Windows sans mot de passe. Vous pouvez utiliser l'authentification unique réelle dans un seul domaine, dans une seule forêt avec plusieurs domaines et dans une configuration à plusieurs forêts et plusieurs domaines.

VMware vous recommande de disposer de deux autorités de certification et de deux serveurs d'inscription déployés pour utiliser l'authentification unique réelle. Les exemples suivants illustrent l'authentification unique réelle dans différentes architectures.

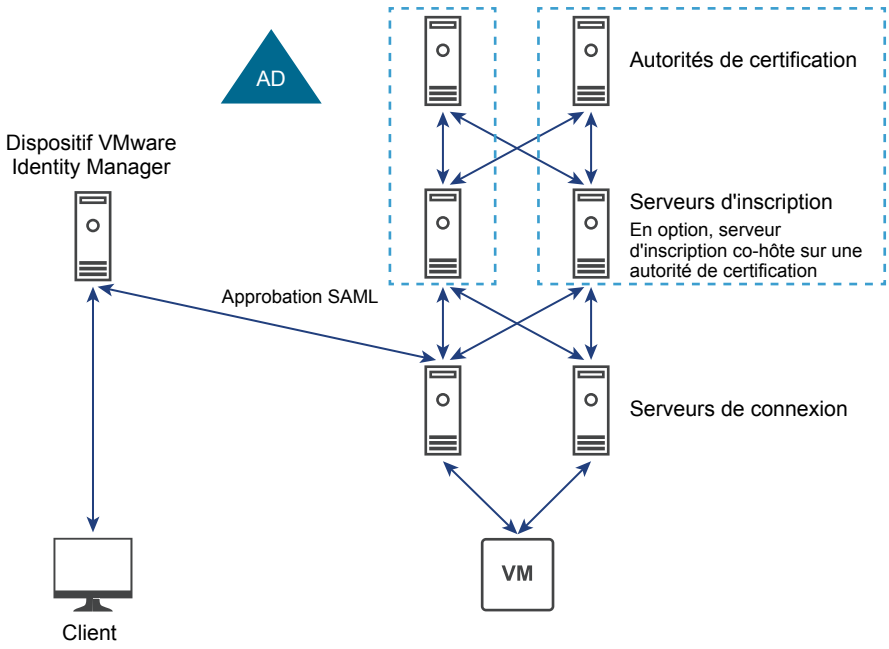
La figure suivante illustre une architecture d'authentification unique réelle simple.

Architecture d'authentification unique réelle très simple



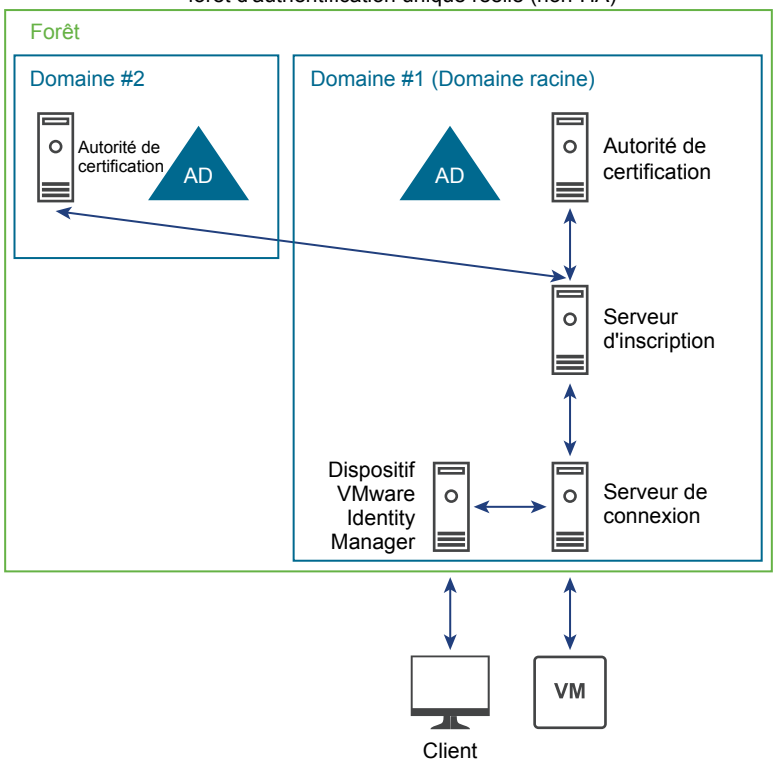
La figure suivante illustre l'authentification unique réelle dans une architecture avec un seul domaine.

Architecture d'authentification unique réelle HA classique (un seul domaine)

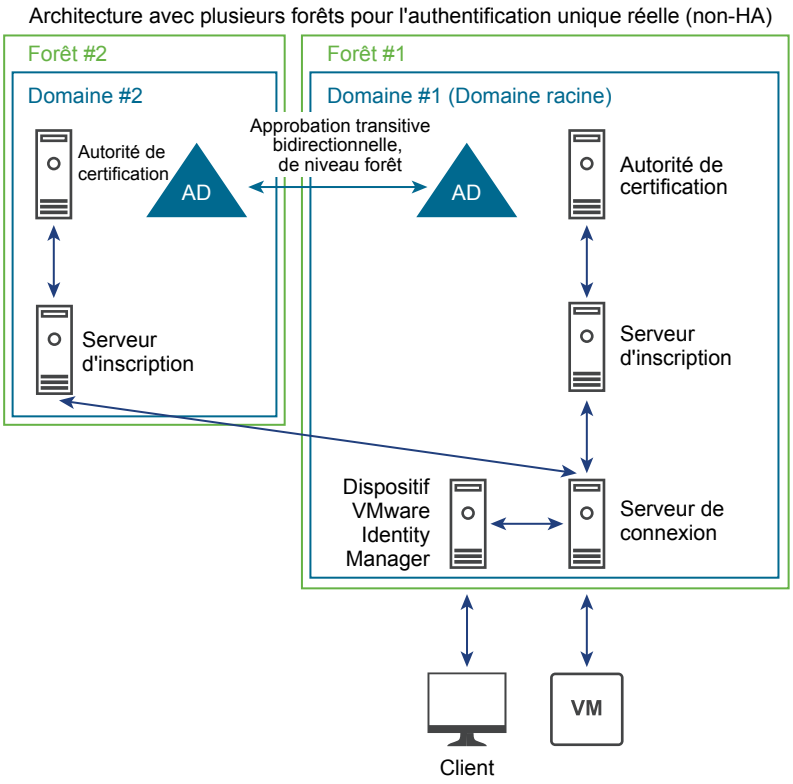


La figure suivante illustre l'authentification unique réelle dans une architecture avec une seule forêt et plusieurs domaines.

Architecture avec plusieurs domaines et une seule forêt d'authentification unique réelle (non-HA)



La figure suivante illustre l'authentification unique réelle dans une architecture avec plusieurs forêts.



Configurer une autorité de certification d'entreprise

Si une autorité de certification n'est pas déjà configurée, vous devez ajouter le rôle Services de certificats Active Directory (AD CS) à un serveur Windows et configurer le serveur pour qu'il soit une autorité de certification d'entreprise.

Si une autorité de certification d'entreprise est déjà configurée, vérifiez que vous utilisez les paramètres décrits dans cette procédure.

Vous devez disposer d'au moins une autorité de certification d'entreprise, et VMware vous recommande d'en avoir deux pour le basculement et l'équilibrage de charge. Le serveur d'inscription que vous créez pour l'authentification unique réelle communique avec l'autorité de certification d'entreprise. Si vous configurez le serveur d'inscription pour qu'il utilise plusieurs autorités de certification d'entreprise, il alternera entre les autorités de certification disponibles. Si vous installez le serveur d'inscription sur la même machine qui héberge l'autorité de certification d'entreprise, vous pouvez configurer le serveur d'inscription pour qu'il utilise l'autorité de certification locale. Cette configuration est recommandée pour de meilleures performances.

Une partie de cette procédure implique d'activer le traitement non persistant des certificats. Par défaut, le traitement des certificats inclut le stockage d'un enregistrement de chaque demande de certificat et de chaque certificat émis dans la base de données d'autorité de certification. Un volume élevé maintenu de demandes augmente le taux de croissance de la base de données d'autorité de certification et peut consommer tout l'espace disque disponible s'il n'est pas surveillé. Activer le traitement non persistant des certificats peut réduire le taux de croissance de la base de données d'autorité de certification et la fréquence des tâches de gestion de la base de données.

Prérequis

- Créez une machine virtuelle Windows Server 2008 R2 ou Windows Server 2012 R2.

- Vérifiez que la machine virtuelle fait partie du domaine Active Directory pour le déploiement d'Horizon 7.
- Vérifiez que vous utilisez un environnement IPv4. Cette fonctionnalité n'est pas actuellement prise en charge dans un environnement IPv6.
- Vérifiez que le système dispose d'une adresse IP statique.

Procédure

1 Connectez-vous au système d'exploitation de la machine virtuelle en tant qu'administrateur et démarrez le gestionnaire de serveurs.

2 Sélectionnez les paramètres pour ajouter des rôles.

Système d'exploitation	Sélections
Windows Server 2012 R2	a Sélectionnez **Ajouter des rôles et des fonctionnalités**. b Sur la page Sélectionner un type d'installation, sélectionnez **Installation basée sur des rôles ou des fonctionnalités**. c Sur la page Sélectionner le serveur de destination, sélectionnez un serveur.
Windows Server 2008 R2	a Sélectionnez **Rôles** dans l'arborescence de navigation. b Cliquez sur **Ajouter des rôles** pour démarrer l'assistant Ajouter un rôle.

3 Sur la page Sélectionner des rôles de serveurs, sélectionnez **Services de certificats Active Directory**.

4 Dans l'assistant Ajouter des rôles et des fonctionnalités, cliquez sur **Ajouter des fonctionnalités** et laissez la case **Inclure les outils de gestion** cochée.

5 Sur la page Sélectionner les fonctionnalités, acceptez les valeurs par défaut.

6 Sur la page Sélectionner des services de rôle, sélectionnez **Autorité de certification**.

7 Suivez les invites et terminez l'installation.

8 Lorsque l'installation est terminée, sur la page Progression de l'installation, cliquez sur le lien **Configurer les services de certificats Active Directory sur le serveur de destination** pour ouvrir l'assistant Configuration des services de certificats Active Directory.

9 Sur la page Informations d'identification, cliquez sur **Suivant** et remplissez les pages de l'assistant Configuration des services de certificats Active Directory, comme décrit dans le tableau suivant.

Option	Action
Services de rôle	Sélectionnez **Autorité de certification** et cliquez sur **Suivant** (plutôt que sur **Configurer**).
Type d'installation	Sélectionnez **Autorité de certification d'entreprise**.
Type d'autorité de certification	Sélectionnez **Autorité de certification racine** ou **Autorité de certification secondaire**. Certaines entreprises préfèrent le déploiement PKI à deux niveaux. Pour plus d'informations, consultez http://social.technet.microsoft.com/wiki/contents/articles/15037.ad-cs-step-by-step-guide-two-tier-pki-hierarchy-deployment.aspx.
Clé privée	Sélectionnez **Créer une nouvelle clé privée**.
Chiffrement pour l'autorité de certification	Pour l'algorithme de hachage, vous pouvez sélectionner **SHA1**, **SHA256**, **SHA384** ou **SHA512**. Pour la longueur de clé, vous pouvez sélectionner **1024**, **2048**, **3072** ou **4096**. VMware recommande au minimum SHA256 et une clé 2048.
Nom de l'autorité de certification	Acceptez le nom par défaut ou modifiez le nom.

Option	Action
Période de validité	Acceptez la valeur par défaut de 5 ans.
Base de données de certificats	Acceptez les valeurs par défaut.

10 Sur la page Confirmation, cliquez sur **Configurer** et, lorsque l'assistant indique que la configuration est réussie, fermez-le.

11 Ouvrez une invite de commande et entrez la commande suivante afin de configurer l'autorité de certification pour le traitement non persistant des certificats :

```
certutil –setreg DBFlags +DBFLAGS_ENABLEVOLATILEREQUESTS
```

12 Entrez la commande suivante pour ignorer les erreurs de liste de révocation des certificats hors ligne sur l'autorité de certification :

```
certutil –setreg ca\CRLFlags +CRLF_REVCHECK_IGNORE_OFFLINE
```

Cet indicateur est requis, car le certificat racine que l'authentification unique réelle utilise sera en général hors ligne, donc la vérification de la révocation échouera, ce qui est attendu.

13 Entrez les commandes suivantes pour redémarrer le service :

```
sc stop certsvc
sc start certsvc
```

Suivant

Créez un modèle de certificat. Reportez-vous à la section « Créer des modèles de certificat utilisés avec l'authentification unique réelle », page 91.

Créer des modèles de certificat utilisés avec l'authentification unique réelle

Vous devez créer un modèle de certificat pouvant être utilisé pour l'émission de certificats de courte durée et vous devez spécifier quels ordinateurs dans le domaine peuvent demander ce type de certificat.

Vous pouvez créer plusieurs modèles de certificat, mais vous ne pouvez configurer qu'un seul modèle à utiliser à la fois.

Prérequis

- Vérifiez que vous disposez d'une autorité de certification d'entreprise pour créer le modèle décrit dans cette procédure. Reportez-vous à la section « Configurer une autorité de certification d'entreprise », page 89.
- Vérifiez que vous avez préparé Active Directory pour l'authentification par carte à puce. Pour plus d'informations, consultez le document *Installation de View*.
- Créez un groupe de sécurité dans le domaine et la forêt pour les serveurs d'inscription et ajoutez les comptes d'ordinateur des serveurs d'inscription à ce groupe.

Procédure

1 Sur la machine que vous utilisez pour l'autorité de certification, connectez-vous au système d'exploitation en tant qu'administrateur et accédez à **Outils d'administration > Autorité de certification**.

2 Développez l'arborescence dans le volet de gauche, cliquez avec le bouton droit sur **Modèles de certificat** et sélectionnez **Gérer**.

3 Cliquez avec le bouton droit sur le modèle **Connexion de carte à puce** et sélectionnez **Dupliquer**.

4 Apportez les modifications suivantes dans les onglets suivants :

Onglet	Action
Onglet Compatibilité	■ Pour **Autorité de certification**, sélectionnez **Windows Server 2008 R2**. ■ Pour **Destinataire du certificat**, sélectionnez **Windows 7/Windows Server 2008 R2**.
Onglet Général	■ Passez le nom complet du modèle sur **`Authentification unique réelle`**. ■ Modifiez la période de validité sur une période aussi longue qu'un jour de travail classique ; c'est-à-dire aussi longtemps que l'utilisateur peut rester connecté au système. Pour que l'utilisateur ne perde pas son accès aux ressources du réseau lorsqu'il est connecté, la période de validité doit être plus longue que la durée de renouvellement Kerberos TGT dans le domaine de l'utilisateur. (La durée de vie maximale par défaut du ticket est de 10 heures. Pour trouver la stratégie de domaine par défaut, vous pouvez accéder à **Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de compte > Stratégie Kerberos : durée de vie maximale du ticket d'utilisateur**.) ■ Passez la période de renouvellement sur 1 jour.
Onglet Traitement de la demande	■ Pour **Objet**, sélectionnez **Signature et ouverture de session avec carte à puce**. ■ Sélectionnez **Pour le renouvellement automatique des cartes à puce, …**
Onglet Chiffrement	■ Pour **Catégorie de fournisseur**, sélectionnez **Fournisseur de stockage de clés**. ■ Pour **Nom d'algorithme**, sélectionnez **RSA**.
Onglet Serveur	Sélectionnez **Ne pas stocker les certificats et les demandes dans la base de données d'autorité de certification**. **Important** Veillez à désélectionner **Ne pas inclure d'informations de révocation dans les certificats émis**. (Cette case est cochée lorsque vous cochez la première et vous devez la décocher.)
Onglet Conditions d'émission	■ Sélectionnez **Ce nombre de signatures autorisées** et saisissez **1** dans la case. ■ Pour **Type de stratégie**, sélectionnez **Stratégie d'application** et définissez la stratégie sur **Agent de demande de certificat**. ■ Pour **Exiger les éléments suivants pour la réinscription**, sélectionnez **Certificat existant valide**.
Onglet Sécurité	Pour le groupe de sécurité que vous avez créé pour les comptes d'ordinateur du serveur d'inscription, comme décrit dans les conditions préalables, fournissez les autorisations suivantes : Lecture, Inscription a Cliquez sur **Ajouter**. b Spécifiez les ordinateurs qui pourront inscrire des certificats. c Pour ces ordinateurs, cochez les cases appropriées pour leur accorder les autorisations suivantes : Lecture, Inscription.

5 Cliquez sur **OK** dans la boîte de dialogue Propriétés du nouveau modèle.

6 Fermez la fenêtre Console des modèles de certificat.

7 Cliquez avec le bouton droit sur **Modèles de certificat** et sélectionnez **Nouveau > Modèle de certificat à délivrer**.

Remarque Cette étape est requise pour toutes les autorités de certification qui émettent des certificats en fonction de ce modèle.

8 Dans la fenêtre Activer les modèles de certificat, sélectionnez le modèle que vous venez de créer (par exemple, **Modèle d'authentification unique réelle**) et cliquez sur **OK**.

9 Dans la fenêtre Activer les modèles de certificat, sélectionnez **Ordinateur Agent d'inscription** et cliquez sur **OK**.

Suivant

Créez un service d'inscription. Reportez-vous à la section « Installer et configurer un serveur d'inscription », page 93.

Installer et configurer un serveur d'inscription

Vous exécutez le programme d'installation du Serveur de connexion et vous sélectionnez l'option Serveur d'inscription d'Horizon 7 pour installer un serveur d'inscription. Le serveur d'inscription demande des certificats de courte durée au nom des utilisateurs que vous spécifiez. Ces certificats de courte durée sont le mécanisme que l'authentification unique réelle utilise pour éviter de demander aux utilisateurs de fournir leurs informations d'identification Active Directory.

Vous devez installer et configurer au moins un serveur d'inscription, et le serveur d'inscription ne peut pas être installé sur le même hôte que le Serveur de connexion View. VMware vous recommande de disposer de deux serveurs d'inscription pour le basculement et l'équilibrage de charge. Si vous disposez de deux serveurs d'inscription, par défaut, l'un est préféré et l'autre est utilisé pour le basculement. Toutefois, vous pouvez modifier ce paramètre par défaut pour que le serveur de connexion alterne l'envoi des demandes de certificat aux deux serveurs d'inscription.

Si vous installez le serveur d'inscription sur la même machine qui héberge l'autorité de certification d'entreprise, vous pouvez configurer le serveur d'inscription pour qu'il utilise l'autorité de certification locale. Pour de meilleures performances, VMware recommande de combiner la configuration pour préférer l'utilisation de l'autorité de certification locale et la configuration pour équilibrer la charge des serveurs d'inscription. Ainsi, lorsque les demandes de certificat arrivent, le serveur de connexion utilisera d'autres serveurs d'inscription, et chaque serveur d'inscription traitera les demandes à l'aide de l'autorité de certification locale. Pour plus d'informations sur les paramètres de configuration à utiliser, reportez-vous aux sections « Paramètres de configuration du serveur d'inscription », page 106 et « Paramètres de configuration du Serveur de connexion », page 107.

Prérequis

- Créez une machine virtuelle Windows Server 2008 R2 ou Windows Server 2012 R2 avec au moins 4 Go de mémoire, ou bien utilisez la machine virtuelle qui héberge l'autorité de certification d'entreprise. N'utilisez pas une machine qui est un contrôleur de domaine.
- Vérifiez qu'aucun autre composant View, notamment le Serveur de connexion View, View Composer, le serveur de sécurité, Horizon Client, View Agent ou Horizon Agent, n'est installé sur la machine virtuelle.
- Vérifiez que la machine virtuelle fait partie du domaine Active Directory pour le déploiement d'Horizon 7.
- Vérifiez que vous utilisez un environnement IPv4. Cette fonctionnalité n'est pas actuellement prise en charge dans un environnement IPv6.
- VMware recommande que le système ait une adresse IP statique.
- Vérifiez que vous pouvez vous connecter au système d'exploitation en tant qu'utilisateur de domaine avec des privilèges d'administrateur. Vous devez vous connecter en tant qu'administrateur pour exécuter le programme d'installation.

Procédure

1 Sur la machine que vous prévoyez d'utiliser pour le serveur d'inscription, ajoutez le composant logiciel enfichable Certificat à MMC :

   a Ouvrez la console MMC et sélectionnez **Fichier > Ajouter/Supprimer un composant logiciel enfichable**

   b Sous **Composants logiciels enfichables disponibles**, sélectionnez **Certificats** et cliquez sur **Ajouter**.

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

   d Dans la fenêtre Ajouter ou supprimer des composants logiciels enfichables, cliquez sur **OK**.

2 Émettez un certificat d'agent d'inscription :

   a Dans la console Certificats, développez l'arborescence racine de la console, cliquez avec le bouton droit sur le dossier **Personnel** et sélectionnez **Toutes les tâches > Demander un nouveau certificat**.

   b Dans l'assistant Inscription de certificat, acceptez les valeurs par défaut jusqu'à ce que vous atteigniez la page Demander des certificats.

   c Sur la page Demander des certificats, cochez la case **Agent d'inscription (ordinateur)** et cliquez sur **Inscrire**.

   d Acceptez les valeurs par défaut sur les autres pages de l'assistant et cliquez sur **Terminer** sur la dernière page.

   Dans la console MMC, si vous développez le dossier **Personnel** et sélectionnez **Certificats** dans le volet de gauche, vous voyez un nouveau certificat répertorié dans le volet de droite.

3 Installez le serveur d'inscription :

   a Téléchargez le fichier du programme d'installation du Serveur de connexion View sur le site de téléchargement VMware, à l'adresse https://my.vmware.com/web/vmware/downloads.

   Sous Desktop & End-User Computing, sélectionnez le téléchargement de VMware Horizon 7, qui inclut le Serveur de connexion View.

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

   b Double-cliquez sur le fichier du programme d'installation pour démarrer l'assistant et suivez les invites jusqu'à ce que vous atteigniez la page Options d'installation.

   c Sur la page Options d'installation, sélectionnez **Serveur d'inscription d'Horizon 7** et cliquez sur **Suivant**.

   d Suivez les invites pour terminer l'installation.

   Vous devez activer les connexions entrantes sur le port 32111 (TCP) pour que le serveur d'inscription soit fonctionnel. Le programme d'installation ouvre le port par défaut lors de l'installation.

Suivant

- Si vous avez installé le serveur d'inscription sur la même machine qui héberge une autorité de certification d'entreprise, configurez le serveur d'inscription pour qu'il utilise l'autorité de certification locale. Reportez-vous à la section « Paramètres de configuration du serveur d'inscription », page 106.
- Si vous installez et configurez plusieurs serveurs d'inscription, configurez des serveurs de connexion pour activer l'équilibrage de charge entre les serveurs d'inscription. Reportez-vous à la section « Paramètres de configuration du Serveur de connexion », page 107.
- Couplez des serveurs de connexion avec des serveurs d'inscription. Reportez-vous à la section « Exporter le certificat Client de service d'inscription », page 95.

Exporter le certificat Client de service d'inscription

Pour réaliser le couplage, vous pouvez utiliser le composant logiciel enfichable Certificats MMC afin d'exporter le certificat Client de service d'inscription auto-signé et généré automatiquement depuis un serveur de connexion dans le cluster. Ce certificat est appelé certificat client, car le serveur de connexion est un client du service d'inscription fourni par le serveur d'inscription.

Le service d'inscription doit approuver le Serveur de connexion de VMware Horizon View lorsqu'il invite les serveurs d'inscription à émettre les certificats de courte durée pour les utilisateurs d'Active Directory. Par conséquent, les clusters ou les espaces du Serveur de connexion de VMware Horizon View doivent être couplés avec des serveurs d'inscription.

Le certificat Client de service d'inscription est créé automatiquement lorsqu'un Serveur de connexion Horizon 7 ou version ultérieure est installé et que le service Serveur de connexion de VMware Horizon View démarre. Le certificat est distribué via View LDAP vers d'autres Serveurs de connexion Horizon 7 qui sont ajoutés au cluster ultérieurement. Le certificat est ensuite stocké dans un conteneur personnalisé (`VMware Horizon View Certificates\Certificates`) dans le magasin de certificats Windows sur l'ordinateur.

Prérequis

Vérifiez que vous disposez d'un Serveur de connexion Horizon 7 ou version ultérieure. Pour obtenir des instructions d'installation, consultez le document *Installation de View*. Pour obtenir des instructions de mise à niveau, consultez le document *Mises à niveau de View*.

Important Les clients peuvent utiliser leurs propres certificats pour le couplage, au lieu d'utiliser le certificat généré automatiquement créé par le serveur de connexion. Pour cela, placez le certificat de votre choix (et la clé privée associée) dans le conteneur personnalisé (`VMware Horizon View Certificates\Certificates`) dans le magasin de certificats Windows sur la machine du serveur de connexion. Vous devez ensuite définir le nom convivial du certificat sur **`vdm.ec.new`** et redémarrer le serveur. Les autres serveurs dans le cluster extrairont ce certificat depuis LDAP. Vous pouvez ensuite réaliser les étapes de cette procédure.

Procédure

1 Sur l'une des machines du serveur de connexion dans le cluster, ajoutez le composant logiciel enfichable Certificats à MMC :

   a Ouvrez la console MMC et sélectionnez **Fichier > Ajouter/Supprimer un composant logiciel enfichable**

   b Sous **Composants logiciels enfichables disponibles**, sélectionnez **Certificats** et cliquez sur **Ajouter**.

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

   d Dans la fenêtre Ajouter ou supprimer des composants logiciels enfichables, cliquez sur **OK**.

2 Dans la console MMC, dans le volet de gauche, développez le dossier **Certificats VMware Horizon View** et sélectionnez le dossier **Certificats**.

3 Dans le volet de droite, cliquez avec le bouton droit sur le fichier de certificat avec le nom convivial **vdm.ec** et sélectionnez **Toutes les tâches > Exporter**.

4 Dans l'assistant Exportation du certificat, acceptez les valeurs par défaut et laissez le bouton radio **Non, ne pas exporter la clé privée** sélectionné.

5 Lorsque vous êtes invité à nommer le fichier, tapez un nom de fichier tel que **`EnrollClient`**, pour le certificat Client de service d'inscription, et suivez les invites pour terminer l'exportation du certificat.

Suivant

Importez le certificat dans le serveur d'inscription. Reportez-vous à la section « Importer le certificat Client de service d'inscription sur le serveur d'inscription », page 96.

Importer le certificat Client de service d'inscription sur le serveur d'inscription

Pour terminer le processus de couplage, vous utilisez le composant logiciel enfichable Certificats MMC afin d'importer le certificat Client de service d'inscription dans le serveur d'inscription. Vous devez effectuer cette procédure sur chaque serveur d'inscription.

Prérequis

- Vérifiez que vous disposez d'un serveur d'inscription Horizon 7 ou version ultérieure. Reportez-vous à la section « Installer et configurer un serveur d'inscription », page 93.
- Vérifiez que vous disposez du bon certificat à importer. Vous pouvez utiliser votre propre certificat ou le certificat Client de service d'inscription auto-signé et généré automatiquement depuis un serveur de connexion dans le cluster, comme décrit dans « Exporter le certificat Client de service d'inscription », page 95.

Important Pour utiliser vos propres certificats pour le couplage, placez le certificat de votre choix (et la clé privée associée) dans le conteneur personnalisé (`VMware Horizon View Certificates\Certificates`) dans le magasin de certificats Windows sur la machine du Serveur de connexion. Vous devez ensuite définir le nom convivial du certificat sur **`vdm.ec.new`** et redémarrer le serveur. Les autres serveurs dans le cluster extrairont ce certificat depuis LDAP. Vous pouvez ensuite réaliser les étapes de cette procédure.

Si vous disposez de votre propre certificat client, le certificat que vous devez copier sur le serveur d'inscription est le certificat racine utilisé pour générer le certificat client.

Procédure

1 Copiez le fichier de certificat approprié sur la machine du serveur d'inscription.

   Pour utiliser le certificat généré automatiquement, copiez le certificat Client de service d'inscription depuis le serveur de connexion. Pour utiliser votre propre certificat, copiez le certificat racine qui a été utilisé pour générer le certificat client.

2 Sur le serveur d'inscription, ajoutez le composant logiciel enfichable Certificats à MMC :

   a Ouvrez la console MMC et sélectionnez **Fichier > Ajouter/Supprimer un composant logiciel enfichable**

   b Sous **Composants logiciels enfichables disponibles**, sélectionnez **Certificats** et cliquez sur **Ajouter**.

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

   d Dans la fenêtre Ajouter ou supprimer des composants logiciels enfichables, cliquez sur **OK**.

3 Dans la console MMC, dans le volet de gauche, cliquez avec le bouton droit sur le dossier **Racines de confiance du serveur d'inscription de VMware Horizon View** et sélectionnez **Toutes les tâches > Importer**.

4 Dans l'assistant Importation du certificat, suivez les invites pour accéder et ouvrir le fichier de certificat **EnrollClient**.

5 Suivez les invites et acceptez les valeurs par défaut pour terminer l'importation du certificat.

6 Cliquez avec le bouton droit sur le certificat importé et ajoutez un nom convivial tel que **vdm.ec** (pour le certificat Client d'inscription).

VMware vous recommande d'utiliser un nom convivial qui identifie le cluster View, mais vous pouvez utiliser n'importe quel nom qui vous permet d'identifier facilement le certificat client.

Suivant

Configurez l'authentificateur SAML utilisé pour déléguer l'authentification à VMware Identity Manager. Reportez-vous à la section « Configurer l'authentification SAML pour l'utiliser avec l'authentification unique réelle », page 97.

Configurer l'authentification SAML pour l'utiliser avec l'authentification unique réelle

Avec la fonctionnalité d'authentification unique réelle introduite dans Horizon 7, les utilisateurs peuvent se connecter à VMware Identity Manager 2.6 et versions ultérieures à l'aide de l'authentification par carte à puce, RADIUS ou RSA SecurID. Ils ne seront plus invités à entrer leurs informations d'identification Active Directory, même lorsqu'ils lancent une application ou un poste de travail distant pour la première fois.

Avec les versions antérieures, l'authentification unique fonctionnait en invitant les utilisateurs à entrer leurs informations d'identification Active Directory la première fois qu'ils lançaient un poste de travail distant ou une application publiée s'ils ne s'étaient pas précédemment authentifiés avec leurs informations d'identification Active Directory. Les informations d'identification étaient ensuite mises en cache pour que les lancements suivants ne demandent pas aux utilisateurs d'entrer de nouveau leurs informations d'identification. Avec l'authentification unique réelle, des certificats de courte durée sont créés et utilisés à la place des informations d'identification AD.

Même si le processus de configuration de l'authentification SAML pour VMware Identity Manager n'a pas changé, une étape supplémentaire a été ajoutée pour l'authentification unique réelle. Vous devez configurer VMware Identity Manager pour que les fenêtres contextuelles de mot de passe soient supprimées.

Remarque Si votre déploiement inclut plusieurs instances du Serveur de connexion View, vous devez associer l'authentificateur SAML à chaque instance.

Prérequis

- Vérifiez que l'authentification unique est activée comme paramètre global. Dans View Administrator, sélectionnez **Configuration > Paramètres généraux** et vérifiez que **Single sign-on (SSO)** est défini sur **Activé**.
- Vérifiez qu'VMware Identity Manager est installé et configuré. Consultez la documentation de VMware Identity Manager disponible à l'adresse suivante : https://www.vmware.com/support/pubs/vidm_pubs.html
- Vérifiez que le certificat racine de l'autorité de certification de signature pour le certificat du serveur SAML est installé sur l'hôte du serveur de connexion. VMware recommande de ne pas configurer d'authentificateurs SAML pour utiliser des certificats auto-signés. Consultez la rubrique « Importer un certificat racine et des certificats intermédiaires dans un magasin de certificats Windows » du chapitre « Configuration de certificats SSL pour des serveurs View » dans le document *Installation de View*.
- Notez le FQDN de l'instance du serveur VMware Identity Manager.

Procédure

1 Dans Horizon Administrator, sélectionnez **Configuration > Serveurs**.

2 Dans l'onglet **Serveurs de connexion**, sélectionnez une instance du serveur à associer à l'authentificateur SAML et cliquez sur **Modifier**.

3 Dans l'onglet **Authentification**, dans le menu déroulant **Délégation de l'authentification à VMware Horizon (authentificateur SAML 2.0)**, sélectionnez **Autorisée** ou **Requise**.

Vous pouvez configurer chaque instance du Serveur de connexion View dans votre déploiement pour disposer de paramètres d'authentification SAML différents, adaptés à vos exigences.

4 Cliquez sur **Gérer des authentificateurs SAML**, puis sur **Ajouter**.

5 Configurez l'authentificateur SAML dans la boîte de dialogue Ajouter un authentificateur SAML 2.0.

Option	Description
Étiquette	Vous pouvez utiliser le FQDN de l'instance du serveur VMware Identity Manager.
Description	(Facultatif) Vous pouvez utiliser le FQDN de l'instance du serveur VMware Identity Manager.
URL de métadonnées	URL pour récupérer toutes les informations requises pour échanger des informations SAML entre le fournisseur d'identité SAML et l'instance du Serveur de connexion View. Dans l'URL `https://<NOM DE VOTRE OCCURRENCE HORIZON SERVER>/SAAS/API/1.0/GET/metadata/idp.xml`, cliquez sur **<NOM DE VOTRE OCCURRENCE HORIZON SERVER>** et remplacez-le par le FQDN de l'instance du serveur VMware Identity Manager.
URL d'administration	URL pour accéder à la console d'administration du fournisseur d'identité SAML (instance VMware Identity Manager). Cette URL a le format **`https://<Identity-Manager-FQDN>:8443.`**

6 Cliquez sur **OK** pour enregistrer la configuration de l'authentificateur SAML.

Si vous avez fourni des informations valides, vous devez accepter le certificat auto-signé (non recommandé) ou utiliser un certificat approuvé pour View et VMware Identity Manager.

Le menu déroulant **Authentificateur SAML 2.0** affiche l'authentificateur récemment créé qui est maintenant défini comme l'authentificateur sélectionné.

7 Dans la section Intégrité du système du tableau de bord de View Administrator, sélectionnez **Autres composants > Authentificateurs SAML 2.0**, sélectionnez l'authentificateur SAML que vous avez ajouté, puis vérifiez les détails.

Si la configuration aboutit, la santé de l'authentificateur est représentée par la couleur verte. La santé de l'authentificateur peut s'afficher en rouge si le certificat n'est pas approuvé, si le service VMware Identity Manager n'est pas disponible ou si l'URL des métadonnées n'est pas valide. Si le certificat n'est pas approuvé, vous pourrez peut-être cliquer sur **Vérifier** pour valider et accepter le certificat.

8 Connectez-vous à la console d'administration VMware Identity Manager, accédez à la page Pools View et cochez la case **Supprimer la fenêtre contextuelle de mot de passe**.

Suivant

- Étendez la période d'expiration des métadonnées du Serveur de connexion View pour que les sessions à distance ne se terminent pas après seulement 24 heures. Reportez-vous à la section « Modifier la période d'expiration des métadonnées du fournisseur de services sur le Serveur de connexion View », page 75.
- Utilisez l'interface de ligne de commande `vdmutil` pour configurer l'authentification unique réelle sur un serveur de connexion. Reportez-vous à la section « Configurer le Serveur de connexion View pour l'authentification unique réelle », page 99.

Pour plus d'informations sur le fonctionnement de l'authentification SAML, reportez-vous à la section « Utilisation de l'authentification SAML », page 71.

Configurer le Serveur de connexion View pour l'authentification unique réelle

Vous pouvez utiliser l'interface de ligne de commande `vdmutil` pour configurer et activer ou désactiver l'authentification unique réelle.

Cette procédure est requise pour être exécutée sur un seul serveur de connexion dans le cluster.

Important Cette procédure utilise uniquement les commandes nécessaires pour activer l'authentification unique réelle. Pour voir une liste de toutes les options de configuration disponibles pour la gestion des configurations d'authentification unique réelle et voir une description de chaque option, reportez-vous à la section « Référence de ligne de commande pour configurer l'authentification unique réelle », page 101.

Prérequis

- Vérifiez que vous pouvez exécuter la commande en tant qu'utilisateur disposant du rôle Administrateurs. Vous pouvez utiliser View Administrator pour attribuer le rôle Administrateurs à un utilisateur. Reportez-vous à la section Chapitre 6, « Configuration d'administration déléguée basée sur des rôles », page 111.
- Vérifiez que vous disposez du nom de domaine complet (FQDN) des serveurs suivants :
  - Serveur de connexion
  - Serveur d'inscription

    Pour plus d'informations, reportez-vous à la section « Installer et configurer un serveur d'inscription », page 93.
  - Autorité de certification d'entreprise

    Pour plus d'informations, reportez-vous à la section « Configurer une autorité de certification d'entreprise », page 89.
- Vérifiez que vous disposez du nom NETBIOS ou du FQDN du domaine.
- Vérifiez que vous avez créé un modèle de certificat. Reportez-vous à la section « Créer des modèles de certificat utilisés avec l'authentification unique réelle », page 91.
- Vérifiez que vous avez créé un authentificateur SAML pour déléguer l'authentification à VMware Identity Manager. Reportez-vous à la section « Configurer l'authentification SAML pour l'utiliser avec l'authentification unique réelle », page 97.

Procédure

1 Sur un serveur de connexion dans le cluster, ouvrez une invite de commande et entrez la commande pour ajouter un serveur d'inscription.

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password
--truesso --environment --add --enrollmentServer enroll-server-fqdn
```

Le serveur d'inscription est ajouté à la liste globale.

2 Entrez la commande pour répertorier les informations pour ce serveur d'inscription.

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password
--truesso --environment --list --enrollmentServer enroll-server-fqdn --domain domain-fqdn
```

La sortie indique le nom de la forêt, si le certificat du serveur d'inscription est valide, le nom et les détails du modèle de certificat que vous pouvez utiliser et le nom commun de l'autorité de certification. Pour configurer les domaines auxquels le serveur d'inscription peut se connecter, vous pouvez utiliser un paramètre de registre Windows sur le serveur d'inscription. L'option par défaut consiste à se connecter à tous les domaines d'approbation.

Important Vous devrez spécifier le nom commun de l'autorité de certification à l'étape suivante.

3 Entrez la commande pour créer un connecteur d'authentification unique réelle, qui contiendra les informations de configuration, et activez le connecteur.

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password
--truesso --create --connector --domain domain-fqdn --template TrueSSO-template-name --
primaryEnrollmentServer enroll-server-fqdn --certificateServer ca-common-name --mode enabled
```

Dans cette commande, *TrueSSO-template-name* est le nom du modèle indiqué dans la sortie de l'étape précédente et *ca-common-name* est le nom commun de l'autorité de certification d'entreprise indiqué dans cette sortie.

Le connecteur d'authentification unique réelle est activé sur un pool ou un cluster pour le domaine spécifié. Pour désactiver l'authentification unique réelle au niveau du pool, exécutez `vdmUtil --certsso --edit --connector <domain> --mode disabled`. Pour désactiver l'authentification unique réelle pour une machine virtuelle individuelle, vous pouvez utiliser GPO (vdm_agent.adm).

4 Entrez la commande pour découvrir les authentificateurs SAML qui sont disponibles.

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password
--truesso --list --authenticator
```

Des authentificateurs sont créés lorsque vous configurez l'authentification SAML entre VMware Identity Manager et un serveur de connexion, à l'aide de View Administrator.

La sortie indique le nom de l'authentificateur et si l'authentification unique réelle est activée.

Important Vous devrez spécifier le nom de l'authentificateur à l'étape suivante.

5 Entrez la commande pour permettre à l'authentificateur d'utiliser le mode Authentification unique réelle.

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password
--truesso --authenticator --edit --name authenticator-fqdn --truessoMode {ENABLED|ALWAYS}
```

Pour `--truessoMode`, utilisez `ENABLED` si vous voulez que l'authentification unique réelle soit utilisée uniquement si aucun mot de passe n'a été fourni lorsque l'utilisateur s'est connecté à VMware Identity Manager. Dans ce cas, si un mot de passe a été utilisé et mis en cache, le système utilisera le mot de passe. Définissez `--truessoMode` sur `ALWAYS` si vous voulez que l'authentification unique réelle soit utilisée même si un mot de passe a été fourni lorsque l'utilisateur s'est connecté à VMware Identity Manager.

Suivant

Dans View Administrator, vérifiez l'état de santé de la configuration d'authentification unique réelle. Pour plus d'informations, reportez-vous à la section « Utilisation du tableau de bord de santé du système pour résoudre des problèmes liés à l'authentification unique réelle », page 108.

Pour configurer des options avancées, utilisez les paramètres avancés Windows sur le système approprié. Reportez-vous à la section « Paramètres de configuration avancée pour l'authentification unique réelle », page 105.

Référence de ligne de commande pour configurer l'authentification unique réelle

Vous pouvez utiliser l'interface de ligne de commande vdmutil pour configurer et gérer la fonctionnalité d'authentification unique réelle.

Emplacement de l'utilitaire

Par défaut, le chemin d'accès vers le fichier exécutable de la commande `vdmutil` est `C:\Program Files\VMware\VMware View\Server\tools\bin`. Pour éviter d'entrer le chemin d'accès sur la ligne de commande, ajoutez-le à la variable d'environnement PATH.

Syntaxe et authentification

Utilisez la forme suivante de la commande `vdmutil` dans une invite de commande Windows.

`vdmutil` *`options d'authentification`* `--truesso` *`options supplémentaires et arguments`*

Les options supplémentaires que vous pouvez utiliser dépendent de l'option de commande. Cette rubrique décrit les options de configuration de l'authentification unique réelle (`--truesso`). Voici un exemple de commande pour répertorier des connecteurs ayant été configurés pour l'authentification unique réelle :

`vdmUtil --authAs` *`admin-role-user`* `--authDomain` *`domain-name`* `--authPassword` *`admin-user-password`* `--truesso --list --connector`

La commande `vdmutil` inclut des options d'authentification pour spécifier le nom d'utilisateur, le domaine et le mot de passe à utiliser pour l'authentification.

Tableau 5-1. options d'authentification de la commande vdmutil

Option	Description
`--authAs`	Nom d'un utilisateur administrateur View. N'utilisez ni le format *domain**username* ni le format de nom principal d'utilisateur (UPN).
`--authDomain`	Nom de domaine complet ou nom Netbios du domaine de l'utilisateur administrateur View spécifié dans l'option `--authAs`.
`--authPassword`	Mot de passe de l'utilisateur administrateur View spécifié dans l'option `--authAs`. Si vous entrez **« * »** plutôt qu'un mot de passe, la commande `vdmutil` affiche une invite de mot de passe et ne conserve pas les mots de passe sensibles dans l'historique des commandes sur la ligne de commande.

Vous devez utiliser les options d'authentification avec toutes les options de la commande `vdmutil`, à l'exception de `--help` et de `--verbose`.

Sortie de commande

La commande `vdmutil` renvoie 0 lorsqu'une opération réussit et un code différent de zéro spécifique d'un échec lorsqu'une opération échoue. La commande `vdmutil` écrit des messages d'erreur en format d'erreur standard. Lorsqu'une opération produit une sortie ou lorsque la journalisation détaillée est activée à l'aide de l'option `--verbose`, la commande `vdmutil` écrit la sortie en format de sortie standard, en anglais américain.

Commandes pour gérer des serveurs d'inscription

Vous devez ajouter un serveur d'inscription pour chaque domaine. Vous pouvez également ajouter un second serveur d'inscription et le désigner ultérieurement comme serveur de sauvegarde.

Pour plus de clarté, les options indiquées dans le tableau suivant ne représentent pas la commande complète que vous devez entrer. Seules les options spécifiques à la tâche particulière sont incluses. Par exemple, une ligne indique les options `--environment --list --enrollmentServers`, mais la commande `vdmUtil` que vous entrez réellement contient également des options pour l'authentification et pour spécifier que vous configurez l'authentification unique réelle :

```
vdmUtil --authAs admin-role-user --authDomain netbios-name --authPassword admin-user-password --
truesso --environment --list --enrollmentServers
```

Pour plus d'informations sur les options d'authentification, reportez-vous à la section « Référence de ligne de commande pour configurer l'authentification unique réelle », page 101.

Tableau 5-2. Options de commande vdmutil truesso pour gérer des serveurs d'inscription

Commande et options	Description
`--environment --add --enrollmentServer` *enroll-server-fqdn*	Ajoute le serveur d'inscription spécifié à l'environnement, où *enroll-server-fqdn* est le nom de domaine complet du serveur d'inscription. Si le serveur d'inscription a déjà été ajouté, rien ne se passe lorsque vous exécutez cette commande.
`--environment --remove --enrollmentServer` *enroll-server-fqdn*	Supprime le serveur d'inscription spécifié de l'environnement, où *enroll-server-fqdn* est le nom de domaine complet du serveur d'inscription. Si le serveur d'inscription a déjà été supprimé, rien ne se passe lorsque vous exécutez cette commande.
`--environment --list --enrollmentServers`	Répertorie les noms de domaine complets de tous les serveurs d'inscription dans l'environnement.
`--environment --list --enrollmentServer` *enroll-server-fqdn*	Répertorie les noms de domaine complets des domaines et des forêts qui sont approuvés par les domaines et les forêts auxquels le serveur d'inscription appartient, et l'état du certificat d'inscription, qui peut être VALID ou INVALID. VALID signifie qu'un certificat d'agent d'inscription est installé sur le serveur d'inscription. L'état peut être INVALID pour plusieurs raisons : ■ Le certificat n'a pas été installé. ■ Le certificat n'est pas encore valide ou il a expiré. ■ Le certificat n'a pas été émis par une autorité de certification d'entreprise de confiance. ■ La clé privée n'est pas disponible. ■ Le certificat a été endommagé. Le fichier journal sur le serveur d'inscription peut fournir la raison de l'état INVALID.
`--environment --list --enrollmentServer` *enroll-server-fqdn* `--domain` *domain-fqdn*	Pour le serveur d'inscription dans le domaine spécifié, répertorie les noms communs des autorités de certification disponibles, et fournit les informations suivantes sur chaque modèle de certificat pouvant être utilisé pour l'authentification unique réelle : nom, longueur de clé minimale et algorithme de hachage.

Commandes pour gérer des connecteurs

Vous créez un connecteur pour chaque domaine. Le connecteur définit les paramètres qui sont utilisés pour l'authentification unique réelle.

Pour plus de clarté, les options indiquées dans le tableau suivant ne représentent pas la commande complète que vous devez entrer. Seules les options spécifiques à la tâche particulière sont incluses. Par exemple, une ligne indique les options `--list --connector`, mais la commande `vdmUtil` que vous entrez réellement contient également des options pour l'authentification et pour spécifier que vous configurez l'authentification unique réelle :

`vdmUtil --authAs` *`admin-role-user`* `--authDomain` *`netbios-name`* `--authPassword` *`admin-user-password`* `--truesso --list --connector`

Pour plus d'informations sur les options d'authentification, reportez-vous à la section « Référence de ligne de commande pour configurer l'authentification unique réelle », page 101.

Tableau 5-3. Options de commande vdmutil truesso pour gérer des connecteurs

Options	Description
`--create --connector --domain` *domain-fqdn* `--template` *template-name* `--primaryEnrollmentServer` *enroll-server1-fqdn* [`--secondaryEnrollmentServer` *enroll-server2-fqdn*] `--certificateServer` *CA-common-name* `--mode {enabled |disabled}`	Crée un connecteur pour le domaine spécifié et configure le connecteur pour utiliser les paramètres suivants : ■ *template-name* est le nom du modèle de certificat à utiliser. ■ *enroll-server1-fqdn* est le FQDN du serveur d'inscription principal à utiliser. ■ *enroll-server2-fqdn* est le FQDN du serveur d'inscription secondaire à utiliser. Ce paramètre est facultatif. ■ *CA-common-name* est le nom commun de l'autorité de certification à utiliser. Il peut s'agir d'une liste d'autorités de certification séparées par une virgule. Pour déterminer le modèle de certificat et l'autorité de certification disponibles pour un serveur d'inscription particulier, vous pouvez exécuter la commande `vdmutil` avec les options `--truesso --environment --list --enrollmentServer` *enroll-server-fqdn* `--domain` *domain-fqdn*.
`--list --connector`	Répertorie les FQDN des domaines sur lesquels un connecteur est déjà créé.
`--list --connector --verbose`	Répertorie tous les domaines avec des connecteurs et, pour chaque connecteur, fournit les informations suivantes : ■ Serveur d'inscription principal ■ Serveur d'inscription secondaire, le cas échéant ■ Nom du modèle de certificat ■ Si le connecteur est activé ou désactivé ■ Nom commun du ou des serveurs d'autorité de certification, s'il y en a plusieurs

Tableau 5-3. Options de commande vdmutil truesso pour gérer des connecteurs (suite)

Options	Description
`--edit --connector` *domain-fqdn* [`--template` *template-name*] [`--mode {enabled |disabled]` [`--primaryEnrollmentServer` *enroll-server1-fqdn*] [`--secondaryEnrollmentServer` *enroll-server2-fqdn*] [`--certificateServer` *CA-common-name*]	Pour le connecteur créé pour le domaine spécifié par *domain-fqdn*, vous permet de modifier les paramètres suivants : ■ *template-name* est le nom du modèle de certificat à utiliser. ■ Le mode peut être `enabled` ou `disabled`. ■ *enroll-server1-fqdn* est le FQDN du serveur d'inscription principal à utiliser. ■ *enroll-server2-fqdn* est le FQDN du serveur d'inscription secondaire à utiliser. Ce paramètre est facultatif. ■ *CA-common-name* est le nom commun de l'autorité de certification à utiliser. Il peut s'agir d'une liste d'autorités de certification séparées par une virgule.
`--delete --connector` *domain-fqdn*	Supprime le connecteur qui a été créé pour le domaine spécifié par *domain-fqdn*.

Commandes pour gérer des authentificateurs

Des authentificateurs sont créés lorsque vous configurez l'authentification SAML entre VMware Identity Manager et un serveur de connexion. La seule tâche de gestion consiste à activer ou désactiver l'authentification unique réelle pour l'authentificateur.

Pour plus de clarté, les options indiquées dans le tableau suivant ne représentent pas la commande complète que vous devez entrer. Seules les options spécifiques à la tâche particulière sont incluses. Par exemple, une ligne indique les options `--list --authenticator`, mais la commande `vdmUtil` que vous entrez réellement contient également des options pour l'authentification et pour spécifier que vous configurez l'authentification unique réelle :

```
vdmUtil --authAs admin-role-user --authDomain netbios-name --authPassword admin-user-password --
truesso --list --authenticator
```

Pour plus d'informations sur les options d'authentification, reportez-vous à la section « Référence de ligne de commande pour configurer l'authentification unique réelle », page 101.

Tableau 5-4. Options de commande vdmutil truesso pour gérer des authentificateurs

Commande et options	Description
`--list --authenticator [--verbose]`	Répertorie les noms de domaine complets (FQDN) de tous les authentificateurs SAML trouvés dans le domaine. Pour chacun, indique si l'authentification unique réelle est activée. Si vous utilisez l'option `--verbose`, les FQDN des serveurs de connexion associés sont également répertoriés.
`--list --authenticator --name` *label*	Pour l'authentificateur spécifié, indique si l'authentification unique réelle est activée et répertorie les FQDN des serveurs de connexion associés. Pour *label*, utilisez l'un des noms répertoriés lorsque vous utilisez l'option `--authenticator` sans l'option `--name`.
`--edit --authenticator --name` *label* `--truessoMode` *mode-value*	Pour l'authentificateur spécifié, définit le mode d'authentification unique réelle sur la valeur que vous indiquez, où *mode-value* peut être l'une des valeurs suivantes : ■ `ENABLED`. L'authentification unique réelle est utilisée uniquement lorsque les informations d'identification Active Directory de l'utilisateur ne sont pas disponibles. ■ `ALWAYS`. L'authentification unique réelle est toujours utilisée même si vIDM dispose des informations d'identification AD de l'utilisateur. ■ `DISABLED`. L'authentification unique réelle est désactivée. Pour *label*, utilisez l'un des noms répertoriés lorsque vous utilisez l'option `--authenticator` sans l'option `--name`.

Paramètres de configuration avancée pour l'authentification unique réelle

Vous pouvez gérer les paramètres avancés pour l'authentification unique réelle en utilisant le modèle GPO sur la machine Horizon Agent, des paramètres de registre sur le serveur d'inscription et des entrées LDAP sur le serveur de connexion. Ces paramètres incluent un délai d'expiration par défaut, configurent l'équilibrage de charge, spécifient les domaines à inclure, etc.

Paramètres de configuration d'Horizon Agent

Vous pouvez utiliser un modèle GPO sur le système d'exploitation agent pour désactiver l'authentification unique réelle au niveau du pool ou pour modifier les valeurs par défaut des paramètres de certificat, tels que la taille de la clé, le nombre et les paramètres des tentatives de reconnexion.

Remarque Le tableau suivant indique les paramètres à utiliser pour configurer l'agent sur des machines virtuelles individuelles, mais vous pouvez également utiliser les fichiers de modèle pour la configuration d'Horizon Agent. Le fichier de modèle d'administration ADMX se nomme (`vdm_agent.admx`). Le fichier de modèle d'administration ADM se nomme (`vdm_agent.adm`). Utilisez les fichiers de modèle pour que ces paramètres de stratégie s'appliquent à toutes les machines virtuelles dans un pool de postes de travail ou d'applications. Si une stratégie est définie, elle est prioritaire sur les paramètres de registre. Dans Horizon 7 version 7.1, les fichiers de modèle d'administration ADM sont obsolètes et les fichiers de modèle d'administration ADMX sont ajoutés.

Les fichiers ADMX sont disponibles dans un fichier groupé `.zip` nommé `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip`, que vous pouvez télécharger sur le site de téléchargement de VMware à l'adresse https://my.vmware.com/web/vmware/downloads. Sous Desktop & End-User Computing, sélectionnez le téléchargement de VMware Horizon 7, qui inclut le fichier groupé `.zip`.

Tableau 5-5. Clés pour configurer l'authentification unique réelle sur Horizon Agent

Clé	Min. et max.	Description
`Disable True SSO`	S/O	Définissez cette clé sur **`true`** pour désactiver la fonctionnalité sur l'agent. Utilisez ce paramètre dans la stratégie de groupe pour désactiver l'authentification unique réelle au niveau du pool. La valeur par défaut est **`false`**.
`Certificate wait timeout`	10 -120	Spécifie le délai d'expiration des certificats pour arriver sur l'agent, en secondes. La valeur par défaut est **`40`**.
`Minimum key size`	1024 - 8192	Taille minimale autorisée pour une clé. La valeur par défaut est **`1024`**, ce qui signifie que, par défaut, si la taille de la clé est inférieure à 1024, la clé ne peut pas être utilisée.
`All key sizes`	S/O	Liste de tailles de clé séparées par une virgule pouvant être utilisées. Il est possible de spécifier 5 tailles au maximum ; par exemple : **`1024,2048,3072,4096`**. La valeur par défaut est **`2048`**.
`Number of keys to pre-create`	1-100	Nombre de clés à créer au préalable sur les serveurs RDS qui fournissent des postes de travail distants et des applications Windows hébergées. La valeur par défaut est **`5`**.
`Minimum validity period required for a certificate`	S/O	Période de validité minimale, en minutes, requise pour qu'un certificat soit réutilisé pour reconnecter un utilisateur. La valeur par défaut est **`5`**.

Paramètres de configuration du serveur d'inscription

Vous pouvez utiliser des paramètres du registre Windows sur le système d'exploitation du serveur d'inscription afin de configurer les domaines auxquels se connecter, divers délais d'expiration, des périodes d'interrogation, des nouvelles tentatives, et si vous préférez utiliser l'autorité de certification qui est installée sur le même serveur local (recommandé).

Pour modifier les paramètres de configuration avancée, vous pouvez ouvrir l'Éditeur du Registre Windows (`regedit.exe`) sur la machine du serveur d'inscription et accéder à la clé de registre suivante :

`HKLM\SOFTWARE\VMware, Inc.\VMware VDM\Enrollment Service`

Tableau 5-6. Clés de registre pour configurer l'authentification unique réelle sur le serveur d'inscription

Clé de Registre	Min. et max.	Type	Description
`ConnectToDomains`	S/O	REG_MULTI_SZ	Liste de domaines auxquels le serveur d'inscription tente de se connecter automatiquement. Pour ce type de registre à chaînes multiples, le nom de domaine complet (FQDN) DNS de chaque domaine est répertorié sur sa propre ligne. L'option par défaut consiste à approuver tous les domaines.
`ExcludeDomains`	S/O	REG_MULTI_SZ	Liste de domaines auxquels le serveur d'inscription ne se connecte pas automatiquement. Si le serveur de connexion fournit une configuration définie avec l'un des domaines, le serveur d'inscription tente de se connecter à ce ou ces domaines. Pour ce type de registre à chaînes multiples, le nom de domaine complet DNS de chaque domaine est répertorié sur sa propre ligne. L'option par défaut consiste à n'exclure aucun domaine.
`ConnectToDomainsInForest`	S/O	REG_SZ	Spécifie s'il faut se connecter et utiliser tous les domaines dans la forêt dont le serveur d'inscription est membre. La valeur par défaut est TRUE. Utilisez l'une des valeurs suivantes : ■ **`0`** signifie faux ; ne vous connectez pas aux domaines de la forêt utilisée. ■ **`!=0`** signifie vrai.
`ConnectToTrustingDomains`	S/O	REG_SZ	Spécifie s'il faut se connecter à des domaines d'approbation/entrants explicitement. La valeur par défaut est TRUE. Utilisez l'une des valeurs suivantes : ■ **`0`** signifie faux ; ne vous connectez pas à des domaines d'approbation/entrants explicitement. ■ **`!=0`** signifie vrai.
`PreferLocalCa`	S/O	REG_SZ	Spécifie s'il faut préférer l'autorité de certification installée localement, si disponible, pour de meilleures performances. Si l'option est définie sur TRUE, le serveur d'inscription enverra les demandes à l'autorité de certification locale. Si la connexion à l'autorité de certification locale échoue, le serveur d'inscription tentera d'envoyer des demandes de certificat à d'autres autorités de certification. La valeur par défaut est FALSE. Utilisez l'une des valeurs suivantes : ■ **`0`** signifie faux. ■ **`!=0`** signifie vrai.

Tableau 5-6. Clés de registre pour configurer l'authentification unique réelle sur le serveur d'inscription (suite)

Clé de Registre	Min. et max.	Type	Description
`MaxSubmitRetryTime`	9500-59000	DWORD	Temps d'attente avant la nouvelle tentative de soumission d'une demande de signature de certificat, en millisecondes. La valeur par défaut est **`25000`**.
`SubmitLatencyWarningTime`	500 - 5000	DWORD	Temps d'avertissement de latence de soumission lorsque l'interface affiche « Dégradé » (en millisecondes). La valeur par défaut est **`1500`**. Le serveur d'inscription utilise ce paramètre pour déterminer si une autorité de certification doit être considérée comme étant dans un état dégradé. Si l'exécution des trois dernières demandes de certificat a mis plus de millisecondes que le nombre spécifié par ce paramètre, l'autorité de certification est considérée comme étant dégradée, et cet état apparaît dans le tableau de bord État de santé de View Administrator. En général, une autorité de certification émet un certificat dans les 20 ms, mais si elle a été inactive pendant quelques heures, toute demande initiale peut prendre un peu plus de temps. Ce paramètre permet à un administrateur de savoir qu'une autorité de certification est lente, sans pour autant qu'elle soit marquée comme étant lente. Utilisez ce paramètre afin de configurer le seuil pour marquer l'autorité de certification comme étant lente.

Paramètres de configuration du Serveur de connexion

Vous pouvez modifier View LDAP sur le Serveur de connexion View afin de configurer un délai d'expiration pour générer des certificats et pour activer ou non les demandes d'équilibrage de charge entre des serveurs d'inscription (recommandé).

Pour modifier les paramètres de configuration avancée, vous devez utiliser l'Éditeur ADSI sur un hôte du Serveur de connexion View. Vous pouvez vous connecter en entrant le nom unique **`DC=vdi, DC=vmware, DC=int`** comme point de connexion et en entrant le nom de serveur et le port de l'ordinateur **`localhost:389`**. Développez **OU=Properties**, sélectionnez **OU=Global** et double-cliquez sur **CN=Common** dans le volet de droite.

Vous pouvez ensuite modifier l'attribut **pae-NameValuePair** pour ajouter une ou plusieurs des valeurs répertoriées dans le tableau suivant. Vous devez utiliser la syntaxe *nom=valeur* lorsque vous ajoutez des valeurs.

Tableau 5-7. Paramètres avancés de l'authentification unique réelle pour les Serveurs de connexion

Clé de Registre	Description
`cs-view-certsso-enable-es-loadbalance=[true|false]`	Indique s'il faut activer les demandes de CSR d'équilibrage de charge entre deux serveurs d'inscription. La valeur par défaut est false. Par exemple, ajoutez `cs-view-certsso-enable-es-loadbalance=true` pour activer l'équilibrage de charge pour que le serveur de connexion utilise d'autres serveurs d'inscription lorsque les demandes de certificat arrivent. Chaque serveur d'inscription peut traiter les demandes à l'aide de l'autorité de certification locale, si le serveur d'inscription et l'autorité de certification se trouvent sur le même hôte.
`cs-view-certsso-certgen-timeout-sec=`*number*	Temps d'attente pour générer un certificat après la réception d'une CSR, en secondes. La valeur par défaut est **`35`**.

Utilisation du tableau de bord de santé du système pour résoudre des problèmes liés à l'authentification unique réelle

Vous pouvez utiliser le tableau de bord de santé du système dans View Administrator pour voir rapidement les problèmes pouvant affecter le fonctionnement de l'authentification unique réelle.

Pour les utilisateurs finaux, si l'authentification unique réelle cesse de fonctionner, lorsque le système tente de connecter l'utilisateur à l'application ou au poste de travail distant, l'utilisateur voit le message suivant : « `Le nom d'utilisateur ou le mot de passe est incorrect.` ». Lorsque l'utilisateur clique sur **OK**, l'écran de connexion s'affiche. Sur l'écran de connexion Windows, l'utilisateur voit une tuile supplémentaire **Utilisateur SSO VMware**. Si l'utilisateur dispose des informations d'identification Active Directory d'un utilisateur autorisé, il peut se connecter avec les informations d'identification AD.

Le tableau de bord de santé du système dans la partie supérieure gauche de l'écran View Administrator contient deux éléments qui concernent l'authentification unique réelle.

Remarque La fonctionnalité d'authentification unique réelle fournit des informations sur le tableau de bord une fois par minute. Cliquez sur l'icône d'actualisation dans le coin supérieur droit pour actualiser les informations immédiatement.

- Vous pouvez cliquer pour développer **Composants View > Authentification unique réelle** et voir une liste des domaines qui utilisent l'authentification unique réelle.

  Vous pouvez cliquer sur un nom de domaine pour voir les informations suivantes : une liste de serveurs d'inscription configurés pour ce domaine, une liste d'autorités de certification d'entreprise, le nom du modèle de certificat utilisé et l'état. S'il y a un problème, le champ État l'explique.

  Pour modifier des paramètres de configuration indiqués dans la boîte de dialogue Détails de domaine de l'authentification unique réelle, utilisez l'interface de ligne de commande `vdmutil` pour modifier le connecteur d'authentification unique réelle. Pour plus d'informations, reportez-vous à la section « Commandes pour gérer des connecteurs », page 103.

- Vous pouvez cliquer pour développer **Autres composants > Authentificateurs SAML 2.0** et voir une liste des authentificateurs SAML qui ont été créés pour déléguer l'authentification à des instances VMware Identity Manager. Vous pouvez cliquer sur le nom de l'authentificateur afin d'examiner les détails et l'état.

Remarque Pour que l'authentification unique réelle soit utilisée, le paramètre global de l'authentification unique doit être activé. Dans View Administrator, sélectionnez **Configuration > Paramètres généraux** et vérifiez que **Single sign-on (SSO)** est défini sur **Activé**.

Tableau 5-8. État de la connexion entre le broker et le serveur d'inscription

Texte d'état	Description
Échec de l'extraction des informations relatives à l'intégrité de l'authentification unique réelle.	Le tableau de bord ne peut pas récupérer les informations sur la santé du broker.
Le serveur d'inscription <FQDN> ne peut pas être contacté par le service de configuration d'authentification unique réelle.	Dans un espace, l'un des brokers est choisi pour envoyer les informations de configuration à tous les serveurs d'inscription utilisés par l'espace. Ce broker actualise la configuration du serveur d'inscription toutes les minutes. Ce message s'affiche si la tâche de configuration n'a pas pu mettre à jour le serveur d'inscription. Pour plus d'informations, consultez le tableau sur la connectivité du serveur d'inscription.
Le serveur d'inscription <FQDN> ne peut pas être contacté pour gérer les sessions sur ce serveur de connexion.	Le broker actuel ne peut pas se connecter au serveur d'inscription. Cet état ne s'affiche que pour le broker vers lequel pointe votre navigateur. S'il y a plusieurs brokers dans l'espace, vous devez modifier votre navigateur pour qu'il pointe vers les autres brokers afin de vérifier leur état. Pour plus d'informations, consultez le tableau sur la connectivité du serveur d'inscription.

Tableau 5-9. Connectivité du serveur d'inscription

Texte d'état	Description
Ce domaine <nom du domaine> n'existe pas sur le serveur d'inscription <FQDN>.	Le connecteur d'authentification unique réelle a été configuré pour utiliser ce serveur d'inscription pour ce domaine, mais le serveur d'inscription n'a pas encore été configuré pour se connecter à ce domaine. Si l'état dure plus d'une minute, vous devez vérifier l'état du broker actuellement responsable de l'actualisation de la configuration de l'inscription.
La connexion du serveur d'inscription <FQDN> au domaine <nom du domaine> est en cours d'établissement.	Le serveur d'inscription n'a pas pu se connecter à un contrôleur de domaine dans ce domaine. Si cet état dure plus d'une minute, vous devrez peut-être vérifier que la résolution de nom entre le serveur d'inscription et le domaine est correcte et qu'il existe une connectivité réseau entre le serveur d'inscription et le domaine.
La connexion du serveur d'inscription <FQDN> au domaine <nom du domaine> est en cours d'arrêt ou dans un état problématique.	Le serveur d'inscription s'est connecté à un contrôleur de domaine dans le domaine, mais il n'a pas pu lire les informations PKI du contrôleur de domaine. Si cela se produit, il existe probablement un problème avec le contrôleur de domaine réel. Ce problème peut également se produire si DNS n'est pas configuré correctement. Consultez le fichier journal sur le serveur d'inscription pour voir quel contrôleur de domaine le serveur d'inscription tente d'utiliser, puis vérifiez que le contrôleur de domaine est complètement opérationnel.
Le serveur d'inscription <FQDN> n'a pas encore lu les propriétés d'inscription d'un contrôleur de domaine.	Cet état est transitoire et ne s'affiche que lors du démarrage du serveur d'inscription, ou lorsqu'un nouveau domaine a été ajouté à l'environnement. En général, cet état dure moins d'une minute. Si cet état dure plus d'une minute, le réseau est extrêmement lent ou il y a un problème provoquant des difficultés à accéder au contrôleur de domaine.
Le serveur d'inscription <FQDN> a lu les propriétés d'inscription au moins une fois, mais il n'a pas pu atteindre un contrôleur de domaine depuis un certain temps.	Tant que le serveur d'inscription lit la configuration PKI d'un contrôleur de domaine, il continue de rechercher les modifications toutes les deux minutes. Cet état sera défini si le contrôleur de domaine (DC) était inaccessible pendant une courte période. En général, cette incapacité à contacter le DC peut signifier que le serveur d'inscription ne peut pas détecter les modifications apportées à la configuration PKI. Tant que les serveurs de certificat peuvent toujours accéder à un contrôleur de domaine, des certificats peuvent toujours être émis.
Le serveur d'inscription <FQDN> a lu les propriétés d'inscription au moins une fois, mais il n'a pas pu atteindre un contrôleur de domaine pendant une période prolongée ou un autre problème existe.	Si le serveur d'inscription n'a pas pu atteindre le contrôleur de domaine pendant une période prolongée, cet état s'affiche. Le serveur d'inscription tente alors de découvrir un autre contrôleur de domaine pour ce domaine. Si un serveur de certificat peut toujours accéder à un contrôleur de domaine, les certificats peuvent toujours être émis, mais si cet état dure plus d'une minute, cela signifie que le serveur d'inscription a perdu l'accès à tous les contrôleurs de domaine pour ce domaine, et il est probable que les certificats ne peuvent plus être émis.

Tableau 5-10. État du certificat d'inscription

Texte d'état	Description
Un certificat d'inscription valide pour la forêt de ce domaine <nom du domaine> n'est pas installé sur le serveur d'inscription <FQDN> ou il est peut-être expiré.	Aucun certificat d'inscription pour ce domaine n'a été installé, ou bien le certificat n'est pas valide ou il a expiré. Le certificat d'inscription doit être émis par une autorité de certification d'entreprise qui est approuvée par la forêt à laquelle appartient ce domaine. Vérifiez que vous avez effectué les étapes dans le document *Administration de View*, qui décrit comment installer le certificat d'inscription sur le serveur d'inscription. Vous pouvez également ouvrir le composant logiciel enfichable de gestion des certificats MMC, en ouvrant le magasin d'ordinateur local. Ouvrez le conteneur de certificat personnel et vérifiez que le certificat est installé et valide. Vous pouvez également ouvrir le fichier journal du serveur d'inscription. Le serveur d'inscription journalisera des informations supplémentaires sur l'état des certificats qu'il trouve.

Tableau 5-11. État du modèle de certificat

Texte d'état	Description
Le modèle <nom> n'existe pas sur le domaine du serveur d'inscription <FQDN>.	Vérifiez que vous avez spécifié le nom de modèle correct.
Les certificats générés par ce modèle ne peuvent PAS être utilisés pour se connecter à Windows.	L'utilisation de carte à puce et la signature de données ne sont pas activées sur ce modèle. Vérifiez que vous avez spécifié le nom de modèle correct. Vérifiez que vous avez effectué les étapes décrites dans la section « Créer des modèles de certificat utilisés avec l'authentification unique réelle », page 91.
Le modèle <nom> est activé pour la connexion par carte à puce, mais il ne peut pas être utilisé.	Ce modèle est activé pour la connexion par carte à puce, mais il ne peut pas être utilisé avec l'authentification unique réelle. Vérifiez que vous avez spécifié le nom de modèle correct et que vous avez effectué toutes les étapes décrites dans la section « Créer des modèles de certificat utilisés avec l'authentification unique réelle », page 91. Vous pouvez également consulter le fichier journal du serveur d'inscription, car il indique le paramètre dans le modèle qui l'empêche d'être utilisé pour l'authentification unique réelle.

Tableau 5-12. État de configuration du serveur de certificat

Texte d'état	Description
Le serveur de certificat <CN de CA> n'existe pas dans le domaine.	Vérifiez que vous avez spécifié le nom correct de l'autorité de certification. Vous devez spécifier le nom commun (CN).
Le certificat ne se trouve pas dans le magasin NTAuth (Enterprise).	Cette autorité de certification n'est pas une autorité de certification d'entreprise ou son certificat d'autorité de certification n'a pas été ajouté au magasin NTAUTH. Si cette autorité de certification n'est pas membre de la forêt, vous devez ajouter manuellement le certificat d'autorité de certification au magasin NTAUTH de cette forêt.

Tableau 5-13. État de connexion du serveur de certificat

Texte d'état	Description
Le serveur d'inscription <FQDN> n'est pas connecté au serveur de certificat <CN de CA>.	Le serveur d'inscription n'est pas connecté au serveur de certificat. Cet état peut être un état transitoire si le serveur d'inscription vient de démarrer ou si l'autorité de certification a été récemment ajoutée à un connecteur d'authentification unique réelle. Si l'état dure plus d'une minute, cela signifie que le serveur d'inscription n'a pas pu se connecter à l'autorité de certification. Vérifiez que cette résolution de nom fonctionne correctement, que vous disposez d'une connectivité réseau à l'autorité de certification et que le compte système du serveur d'inscription a l'autorisation d'accéder à l'autorité de certification.
Le serveur d'inscription <FQDN> s'est connecté au serveur de certificat <CN de CA>, mais ce dernier est dans un état dégradé.	Cet état s'affiche si l'autorité de certification est lente à émettre les certificats. Si l'autorité de certification reste dans cet état, vérifiez sa charge ou les contrôleurs de domaine qu'elle utilise. **Remarque** Si l'autorité de certification a été marquée comme étant lente, elle restera dans cet état jusqu'à ce qu'au moins une demande de certificat soit terminée correctement et que ce certificat ait été émis dans un délai normal.
Le serveur d'inscription <FQDN> peut se connecter au serveur de certificat <CN de CA>, mais le service n'est pas disponible.	Cet état est émis si le serveur d'inscription dispose d'une connexion active vers l'autorité de certification, mais qu'il ne peut pas émettre des certificats. En général, cet état est transitoire. Si l'autorité de certification ne devient pas disponible rapidement, l'état passera sur déconnecté.

Configuration d'administration déléguée basée sur des rôles 6

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 **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 propres à l'objet contrôlent les opérations effectuées sur des types d'objets spécifiques.

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 groupes d'accès pour déléguer l'administration de pools et de batteries de serveurs

Par défaut, des pools de postes de travail automatisés, des pools de postes de travail manuels et des batteries de serveurs sont créés dans le groupe d'accès racine, qui s'affiche sous la forme / ou Root(/) dans View Administrator. Les pools de postes de travail RDS et les pools d'applications héritent du groupe d'accès de leur batterie de serveurs. Vous pouvez créer des groupes d'accès sous le groupe d'accès racine pour déléguer l'administration de pools ou de batteries de serveurs spécifiques à d'autres administrateurs.

Remarque Vous ne pouvez pas directement modifier le groupe d'accès d'un pool de postes de travail RDS ou d'un pool d'applications. Vous devez modifier le groupe d'accès de la batterie de serveurs auquel le pool de postes de travail RDS ou le pool d'applications appartient.

Une machine virtuelle ou physique hérite du groupe d'accès de son pool de postes de travail. Un disque persistant attaché hérite du groupe d'accès de sa machine. Vous pouvez disposer d'un maximum de 100 groupes d'accès, notamment le groupe d'accès racine.

Vous configurez un accès administrateur aux ressources dans un groupe d'accès en attribuant un rôle à un administrateur sur ce groupe d'accès. Les administrateurs ne peuvent accéder qu'aux ressources qui résident dans des groupes d'accès pour lesquels des rôles leur ont été attribués. Le rôle dont un administrateur dispose sur un groupe d'accès détermine le niveau d'accès de l'administrateur sur les ressources de ce groupe d'accès.

Comme les rôles sont hérités du groupe d'accès racine, un administrateur qui dispose d'un rôle sur le groupe d'accès racine détient ce rôle sur tous les groupes d'accès. Les administrateurs qui disposent du rôle Administrateurs sur le groupe d'accès racine sont des super administrateurs, car ils bénéficient d'un accès complet à tous les objets du système.

Un rôle doit contenir au moins un privilège spécifique d'un objet pour s'appliquer à un groupe d'accès. Les rôles ne contenant que des privilèges généraux ne peuvent pas être appliqués aux groupes d'accès.

Vous pouvez utiliser View Administrator pour créer des groupes d'accès et déplacer des pools de postes de travail existants vers des groupes d'accès. Lorsque vous créez un pool de postes de travail automatisé, un pool manuel ou une batterie de serveurs, vous pouvez accepter le groupe d'accès racine par défaut ou sélectionner un autre groupe d'accès.

Remarque Si vous prévoyez de fournir un accès à vos applications et postes de travail via VMware Identity Manager, assurez-vous de créer les pools d'applications et de postes de travail en tant qu'utilisateur disposant du rôle Administrateurs sur le groupe d'accès racine dans View Administrator. Si vous attribuez à l'utilisateur le rôle Administrateurs sur un groupe d'accès autre que le groupe d'accès racine, VMware Identity Manager ne reconnaîtra pas l'authentificateur SAML que vous configurez dans View et vous ne pourrez pas configurer le pool dans VMware Identity Manager.

Différents administrateurs pour différents groupes d'accès

Vous pouvez créer un administrateur différent pour gérer chaque groupe d'accès de votre configuration.

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

Tableau 6-1 montre un exemple de ce type de configuration.

Tableau 6-1. Différents administrateurs pour différents groupes d'accès

Administrateur	Rôle	Groupe d'accès
view-domain.com\Admin1	Administrateurs d'inventaire	`/CorporateDesktops`
view-domain.com\Admin2	Administrateurs d'inventaire	`/DeveloperDesktops`

Dans cet exemple, l'administrateur Admin1 dispose du rôle Administrateurs d'inventaire sur le groupe d'accès nommé `CorporateDesktops`, et l'administrateur Admin2 dispose du rôle Administrateurs d'inventaire sur le groupe d'accès nommé `DeveloperDesktops`..

Différents administrateurs pour un même groupe d'accès

Vous pouvez créer différents administrateurs pour gérer un même groupe d'accès.

Par exemple, si les pools de postes de travail de votre entreprise se trouvent dans un groupe d'accès, vous pouvez créer un administrateur qui peut afficher et modifier ces pools et un autre administrateur qui peut uniquement les afficher.

Tableau 6-2 montre un exemple de ce type de configuration.

Tableau 6-2. Différents administrateurs pour un même groupe d'accès

Administrateur	Rôle	Groupe d'accès
view-domain.com\Admin1	Administrateurs d'inventaire	`/CorporateDesktops`
view-domain.com\Admin2	Administrateurs d'inventaire (lecture seule)	`/CorporateDesktops`

Dans cet exemple, l'administrateur Admin1 dispose du rôle Administrateurs d'inventaire sur le groupe d'accès nommé `CorporateDesktops`, et l'administrateur Admin2 dispose du rôle Administrateurs d'inventaire (lecture seule) sur le même groupe d'accès.

Comprendre les autorisations

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

Les autorisations s'affichent différemment dans View Administrator, selon que vous sélectionnez un utilisateur administrateur ou un groupe d'utilisateurs administrateurs, un groupe d'accès ou un rôle.

Tableau 6-3 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 6-3. Autorisations sous l'onglet Administrateurs et groupes pour Admin 1

Rôle	Groupe d'accès
Administrateurs d'inventaire	`MarketingDesktops`
Administrateurs (lecture seule)	`/`

La première autorisation indique qu'Admin 1 dispose du rôle Administrateur d'inventaire sur le groupe d'accès appelé `MarketingDesktops`. La deuxième autorisation indique qu'Admin 1 dispose du rôle Administrateur (lecture seule) sur le groupe d'accès racine.

Tableau 6-4 montre comment les mêmes autorisations s'affichent dans View Administrator lorsque vous sélectionnez le groupe d'accès `MarketingDesktops`.

Tableau 6-4. Autorisations sous l'onglet Dossiers pour MarketingDesktops

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

La première autorisation est la même que la première autorisation indiquée dans Tableau 6-3. La deuxième autorisation est héritée de la deuxième autorisation indiquée dans Tableau 6-3. Étant donné que les dossiers héritent des autorisations du groupe d'accès racine, Admin1 dispose du rôle Administrateur (lecture seule) sur le groupe d'accès `MarketingDesktops`. Lorsqu'une autorisation est héritée, Oui apparaît dans la colonne Héritée.

Tableau 6-5 montre comment la première autorisation de Tableau 6-3 s'affiche dans View Administrator lorsque vous sélectionnez le rôle Administrateurs d'inventaire.

Tableau 6-5. Autorisations sous l'onglet Rôle pour Inventory Administrators (Administrateurs d'inventaire)

Administrateur	Groupe d'accès
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 Serveur de connexion View. 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.

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 115

  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 116

  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 dispose du rôle d'administrateur sur le groupe d'accès 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 122.
- Familiarisez-vous avec les recommandations pour la création d'utilisateurs administrateurs et de groupes d'administrateurs. Reportez-vous à la section « Meilleures pratiques pour des utilisateurs et des groupes d'administrateurs », page 128.
- Pour affecter un rôle personnalisé à l'administrateur, créez le rôle personnalisé. Reportez-vous à la section « Ajouter un rôle personnalisé », page 121.
- Pour créer un administrateur pouvant gérer des pools de postes de travail spécifiques, créez un groupe d'accès et déplacez les pools de postes de travail vers ce groupe d'accès. Reportez-vous à la section « Gérer et répertorier des groupes d'accès », page 118.

Procédure

1 Dans View Administrator, sélectionnez **Configuration de View > Administrateurs**.

2 Sous l'onglet **Administrateurs et groupes**, cliquez sur **Ajouter un utilisateur ou un groupe**.

3 Cliquez sur **Ajouter**, sélectionnez un ou plusieurs critères de recherche, puis cliquez sur **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 **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 S'applique à un groupe d'accès indique si un rôle s'applique à des groupes d'accès. Seuls les rôles contenant des privilèges spécifiques de l'objet s'appliquent aux groupes d'accès. Les rôles ne contenant que des privilèges généraux ne s'appliquent pas aux groupes d'accès.

Option	Action
Le rôle que vous avez sélectionné s'applique aux groupes d'accès	Sélectionnez un ou plusieurs groupes d'accès et cliquez sur **Suivant**.
Vous souhaitez que le rôle s'applique à tous les groupes d'accès	Sélectionnez le groupe d'accès racine et cliquez sur **Suivant**.

6 Cliquez sur **Terminer** pour créer l'utilisateur ou le groupe d'administrateurs.

Le nouvel utilisateur administrateur ou groupe d'administrateurs s'affiche dans le volet de gauche, et le rôle et le groupe d'accès que vous avez sélectionnés s'affichent dans le volet de droite sous l'onglet **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 dispose du rôle d'administrateur sur le groupe d'accès racine.

Procédure

1 Dans View Administrator, sélectionnez **Configuration de View > Administrateurs**.

2 Sous l'onglet **Administrateurs et groupes**, sélectionnez l'utilisateur ou le groupe d'administrateurs, cliquez sur **Supprimer un utilisateur ou un groupe** et sur **OK**.

L'utilisateur ou le groupe d'administrateurs n'apparaît plus sous l'onglet **Administrateurs et groupes**.

Gérer et consulter des autorisations

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

- Ajouter une autorisation page 116

  Vous pouvez ajouter une autorisation qui inclut un utilisateur administrateur ou un groupe d'administrateurs spécifique, un rôle spécifique ou un groupe d'accès spécifique.

- Supprimer une autorisation page 117

  Vous pouvez supprimer une autorisation qui inclut un utilisateur administrateur ou un groupe d'administrateurs spécifique, un rôle spécifique ou un groupe d'accès spécifique.

- Consulter des autorisations page 118

  Vous pouvez vérifier les autorisations qui incluent un administrateur ou un groupe spécifique, un rôle spécifique ou un groupe d'accès spécifique.

Ajouter une autorisation

Vous pouvez ajouter une autorisation qui inclut un utilisateur administrateur ou un groupe d'administrateurs spécifique, un rôle spécifique ou un groupe d'accès spécifique.

Procédure

1 Dans View Administrator, sélectionnez **Configuration de View > 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 **Administrateurs et groupes**, sélectionnez l'administrateur ou le groupe et cliquez sur **Ajouter une autorisation**. b Sélectionnez un rôle. c Si le rôle ne s'applique pas aux groupes d'accès, cliquez sur **Terminer**. d Si le rôle s'applique aux groupes d'accès, cliquez sur **Suivant**, sélectionnez un ou plusieurs groupes d'accès, puis cliquez sur **Terminer**. Un rôle doit contenir au moins un privilège spécifique à un objet pour s'appliquer à un groupe d'accès.
Create a permission that includes a specific role (Créer une autorisation qui inclut un rôle spécifique)	a Sous l'onglet **Rôles**, sélectionnez le rôle, cliquez sur **Autorisations** puis sur **Ajouter une autorisation**. b Cliquez sur **Ajouter**, sélectionnez un ou plusieurs critères de recherche, puis cliquez sur **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 groupes d'accès, cliquez sur **Terminer**. e Si le rôle s'applique aux groupes d'accès, cliquez sur **Suivant**, sélectionnez un ou plusieurs groupes d'accès, puis cliquez sur **Terminer**. Un rôle doit contenir au moins un privilège spécifique à un objet pour s'appliquer à un groupe d'accès.
Créer une autorisation qui inclut un groupe d'accès spécifique	a Dans l'onglet **Groupes d'accès**, sélectionnez le groupe d'accès et cliquez sur **Ajouter une autorisation**. b Cliquez sur **Ajouter**, sélectionnez un ou plusieurs critères de recherche, puis cliquez sur **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 **Suivant**, sélectionnez un rôle et cliquez sur **Terminer**. Un rôle doit contenir au moins un privilège spécifique à un objet pour s'appliquer à un groupe d'accès.

Supprimer une autorisation

Vous pouvez supprimer une autorisation qui inclut un utilisateur administrateur ou un groupe d'administrateurs spécifique, un rôle spécifique ou un groupe d'accès 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. Du fait qu'au moins un administrateur doit disposer du rôle Administrateur sur le groupe d'accès 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 **Configuration de View > 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 **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 **Rôles**.
Supprimer une autorisation qui s'applique à un groupe d'accès spécifique	Sélectionnez le dossier dans l'onglet **Groupes d'accès**.

3 Sélectionnez l'autorisation et cliquez sur **Supprimer une autorisation**.

Consulter des autorisations

Vous pouvez vérifier les autorisations qui incluent un administrateur ou un groupe spécifique, un rôle spécifique ou un groupe d'accès spécifique.

Procédure

1 Sélectionnez **Configuration de View > 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 **Administrateurs et groupes**.
Review the permissions that include a specific role (Consulter les autorisations qui comportent un rôle spécifique)	Sélectionnez le rôle dans l'onglet **Rôles** et cliquez sur **Autorisations**.
Vérifier les autorisations qui incluent un groupe d'accès spécifique	Sélectionnez le dossier dans l'onglet **Groupes d'accès**.

Gérer et répertorier des groupes d'accès

Vous pouvez utiliser View Administrator pour ajouter et supprimer des groupes d'accès, et pour vérifier les pools de postes de travail et les machines d'un groupe d'accès particulier.

- Ajouter un groupe d'accès page 119

  Vous pouvez déléguer l'administration de machines, de pools de postes de travail ou de batteries de serveurs spécifiques à différents administrateurs en créant des groupes d'accès. Par défaut, les pools de postes de travail, les pools d'applications et les batteries de serveurs résident dans le groupe d'accès racine.

- Déplacer un pool de postes de travail ou une batterie de serveurs vers un autre groupe d'accès page 119

  Après avoir créé un groupe d'accès, vous pouvez déplacer des pools de postes de travail automatisés, des pools manuels ou des batteries de serveurs vers le nouveau groupe d'accès.

- Supprimer un groupe d'accès page 120

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

- Vérifier les pools de postes de travail, les pools d'applications ou les batteries de serveurs d'un groupe d'accès page 120

  Vous pouvez afficher les pools de postes de travail, les pools d'application ou les batteries de serveurs d'un groupe d'accès particulier dans View Administrator.

- Vérifier les machines virtuelles vCenter d'un groupe d'accès page 120

  Vous pouvez afficher dans View Administrator les machines virtuelles vCenter incluses dans un groupe d'accès particulier. Une machine virtuelle vCenter hérite du groupe d'accès de son pool.

Ajouter un groupe d'accès

Vous pouvez déléguer l'administration de machines, de pools de postes de travail ou de batteries de serveurs spécifiques à différents administrateurs en créant des groupes d'accès. Par défaut, les pools de postes de travail, les pools d'applications et les batteries de serveurs résident dans le groupe d'accès racine.

Vous pouvez disposer d'un maximum de 100 groupes d'accès, notamment le groupe d'accès racine.

Procédure

1 Dans View Administrator, accédez à la boîte de dialogue Ajouter un groupe d'accès.

Option	Action
À partir d'un catalogue	■ Sélectionnez **Catalogue > Pools de postes de travail**. ■ Dans le menu déroulant **Groupe d'accès** dans le volet supérieur de la fenêtre, sélectionnez **Nouveau groupe d'accès**.
À partir des ressources	■ Sélectionnez **Ressources > Batteries de serveurs**. ■ Dans le menu déroulant **Groupe d'accès** dans le volet supérieur de la fenêtre, sélectionnez **Nouveau groupe d'accès**.
À partir de la configuration de View	■ Sélectionnez **Configuration de View > Administrateurs**. ■ Dans l'onglet **Groupes d'accès**, sélectionnez **Ajouter un groupe d'accès**.

2 Tapez un nom et une description pour le groupe d'accès et cliquez sur **OK**.

La description est facultative.

Suivant

Déplacez un ou plusieurs objets vers le groupe d'accès.

Déplacer un pool de postes de travail ou une batterie de serveurs vers un autre groupe d'accès

Après avoir créé un groupe d'accès, vous pouvez déplacer des pools de postes de travail automatisés, des pools manuels ou des batteries de serveurs vers le nouveau groupe d'accès.

Procédure

1 Dans View Administrator, sélectionnez **Catalogue > Pools de postes de travail** ou **Ressources > Batteries de serveurs**.

2 Sélectionnez un pool ou une batterie de serveurs.

3 Sélectionnez **Modifier un groupe d'accès** dans le menu déroulant **Groupe d'accès** situé dans le volet de la fenêtre supérieure.

4 Sélectionnez le groupe d'accès, puis cliquez sur **OK**.

View Administrator déplace le pool vers le groupe d'accès que vous avez sélectionné.

Supprimer un groupe d'accès

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

Prérequis

Si le groupe d'accès contient des objets, déplacez ces derniers vers un autre groupe d'accès ou vers le groupe d'accès racine. Reportez-vous à la section « Déplacer un pool de postes de travail ou une batterie de serveurs vers un autre groupe d'accès », page 119.

Procédure

1 Dans View Administrator, sélectionnez **Configuration de View > Administrateurs**.

2 Dans l'onglet **Groupes d'accès**, sélectionnez le groupe d'accès et cliquez sur **Supprimer un groupe d'accès**.

3 Cliquez sur **OK** pour supprimer le groupe d'accès.

Vérifier les pools de postes de travail, les pools d'applications ou les batteries de serveurs d'un groupe d'accès

Vous pouvez afficher les pools de postes de travail, les pools d'application ou les batteries de serveurs d'un groupe d'accès particulier dans View Administrator.

Procédure

1 Dans View Administrator, accédez à la page principale des objets.

Objet	Action
Pools de postes de travail	Sélectionnez **Catalogue > Pools de postes de travail**.
Pools d'applications	Sélectionnez **Catalogue > Pools d'applications**.
Batteries de serveurs	Sélectionnez **Ressources > Batteries de serveurs**.

Par défaut, les objets de tous les groupes d'accès sont affichés.

2 Sélectionnez un groupe d'accès dans le menu déroulant **Groupe d'accès** du volet de la fenêtre principale.

Les objets du groupe d'accès que vous avez sélectionné sont affichés.

Vérifier les machines virtuelles vCenter d'un groupe d'accès

Vous pouvez afficher dans View Administrator les machines virtuelles vCenter incluses dans un groupe d'accès particulier. Une machine virtuelle vCenter hérite du groupe d'accès de son pool.

Procédure

1 Dans View Administrator, sélectionnez **Ressources > Machines**.

2 Sélectionnez l'onglet **Machines virtuelles vCenter**.

Par défaut, les machines virtuelles vCenter de tous les groupes d'accès s'affichent.

3 Sélectionnez un groupe d'accès dans le menu déroulant **Groupe d'accès**.

Les machines virtuelles vCenter du groupe d'accès que vous avez sélectionné s'affichent.

Gérer des rôles personnalisés

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

- Ajouter un rôle personnalisé page 121

  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 121

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

- Supprimer un rôle personnalisé page 122

  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 122.

Procédure

1. Dans View Administrator, sélectionnez **Configuration de View > Administrateurs**.
2. Sous l'onglet **Rôles**, cliquez sur **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 122.

Procédure

1. Dans View Administrator, sélectionnez **Configuration de View > Administrateurs**.
2. Sous l'onglet **Rôles**, sélectionnez le rôle.
3. Cliquez sur **Privilèges** pour afficher les privilèges dans le rôle, puis sur **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 117.

Procédure

1 Dans View Administrator, sélectionnez **Configuration de View > Administrateurs**.

2 Sous l'onglet **Rôles**, sélectionnez le rôle et cliquez sur **Supprimer un rôle**.

Le bouton **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 122

  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 124

  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 aux groupes d'accès.

- Privilèges spécifiques de l'objet page 125

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

- Privilèges internes page 125

  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 6-6 décrit les rôles prédéfinis et indique si un rôle peut s'appliquer à un groupe d'accès.

Tableau 6-6. Rôles prédéfinis dans View Administrator

Rôle	Actions réalisables par l'utilisateur	S'applique à un groupe d'accès
Administrateurs	Effectuer toutes les opérations d'administrateur, y compris la création d'utilisateurs et de groupes d'administrateurs supplémentaires. Dans un environnement Cloud Pod Architecture, les administrateurs disposant de ce rôle peuvent configurer et gérer une fédération d'espaces, et gérer des sessions d'espace distantes. Les administrateurs disposant du rôle Administrateurs sur le groupe d'accès racine sont des super utilisateurs, car ils bénéficient d'un accès complet à tous les objets d'inventaire du système. Comme le rôle Administrators (Administrateurs) contient tous les privilèges, vous devez l'affecter à un ensemble limité d'utilisateurs. Initialement, ce rôle est attribué aux membres du groupe Administrateurs local sur l'hôte de votre Serveur de connexion View sur le groupe d'accès racine. **Important** Un administrateur doit disposer du rôle Administrateurs sur le groupe d'accès racine pour effectuer les tâches suivantes : ■ Ajouter et supprimer des groupes d'accès. ■ Gérer des applications ThinApp et des paramètres de configuration dans View Administrator. ■ Utiliser les commandes `vdmadmin`, `vdmimport` et `lmvutil`.	Oui
Administrateurs (lecture seule)	■ Voir, mais pas modifier, des paramètres généraux et des objets d'inventaire. ■ Voir, mais pas modifier, des applications et des paramètres ThinApp. ■ Exécuter toutes les commandes et utilitaires de ligne de commande PowerShell, notamment `vdmexport`, en excluant toutefois `vdmadmin`, `vdmimport` et `lmvutil`. Dans un environnement Cloud Pod Architecture, les administrateurs disposant de ce rôle peuvent afficher les objets et les paramètres d'inventaire de la couche de données globale. Lorsque les administrateurs disposent de ce rôle sur un groupe d'accès, ils ne peuvent afficher que les objets d'inventaire de ce groupe d'accès.	Oui
Administrateurs d'inscription d'agent	Inscrire des machines non gérées telles que des systèmes physiques, des machines virtuelles autonomes et des hôtes RDS.	Non
Administrateurs de configuration et règles générales	Afficher et modifier des stratégies globales et des paramètres de configuration, à l'exception des rôles et des autorisations d'administrateur, ainsi que des applications et des paramètres ThinApp.	Non
Administrateurs de configuration et règles générales (lecture seule)	Afficher, mais pas modifier, des stratégies globales et des paramètres de configuration, à l'exception des rôles et des autorisations d'administrateur, ainsi que des applications et paramètres ThinApp.	Non
Administrateurs d'inventaire	■ Effectuer toutes les opérations liées aux machines, 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 disposent de ce rôle sur un groupe d'accès, ils ne peuvent effectuer ces opérations que sur les objets d'inventaire de ce groupe d'accès.	Oui

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

Rôle	Actions réalisables par l'utilisateur	S'applique à un groupe d'accès
Administrateurs d'inventaire (lecture seule)	Voir, mais pas modifier, des objets d'inventaire. Lorsque les administrateurs disposent de ce rôle sur un groupe d'accès, ils ne peuvent afficher que les objets d'inventaire de ce groupe d'accès.	Oui
Administrateurs locaux	Effectuer toutes les opérations d'administrateur, à l'exception de la création d'utilisateurs administrateurs et de groupes d'administrateurs supplémentaires. Dans un environnement Cloud Pod Architecture, les administrateurs disposant de ce rôle ne peuvent ni effectuer des opérations sur la couche de données globale ni gérer des sessions sur des espaces distants.	Oui
Administrateurs locaux (lecture seule)	Identique au rôle Administrateurs (lecture seule), à l'exception de l'affichage des objets et des paramètres d'inventaire de la couche de données globale. Les administrateurs disposant de ce rôle bénéficient de droits de lecture seule uniquement sur l'espace local.	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 aux groupes d'accès.

Tableau 6-7 décrit les privilèges généraux et répertorie les rôles prédéfinis qui contiennent chaque privilège.

Tableau 6-7. Privilèges généraux

Privilège	Actions réalisables par l'utilisateur	Rôles prédéfinis
Interaction de console	Ouvrir une session sur et utiliser View Administrator.	Administrateurs Administrateurs (lecture seule) Administrateurs d'inventaire Administrateurs d'inventaire (lecture seule) Administrateurs de configuration et règles générales Administrateurs de configuration et règles générales (lecture seule)
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 Administrateurs dans le groupe d'accès racine pour utiliser les commandes `vdmadmin`, `vdmimport` et `lmvutil`.	Administrateurs Administrateurs (lecture seule)
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.	Administrateurs Administrateurs de configuration et règles générales
Gérer des sessions globales	Gérer les sessions globales dans un environnement Architecture Cloud Pod.	Administrateurs

Tableau 6-7. Privilèges généraux (suite)

Privilège	Actions réalisables par l'utilisateur	Rôles prédéfinis
Gérer des rôles et autorisations	Créer, modifier et supprimer des rôles et des autorisations d'administrateur.	Administrateurs
Inscrire l'agent	Installez Horizon Agent sur des machines non gérées, comme des systèmes physiques, des machines virtuelles autonomes et des hôtes RDS. Lors de l'installation d'Horizon Agent, vous devez fournir des informations d'identification d'ouverture de session d'administrateur pour inscrire la machine non gérée sur l'instance du Serveur de connexion View.	Administrateurs 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 propres aux objets peuvent être appliqués à des groupes d'accès.

Tableau 6-8 décrit les privilèges spécifiques de l'objet. Les rôles prédéfinis Administrators (Administrateurs) et Inventory Administrators (Administrateurs d'inventaire) contiennent tous les privilèges.

Tableau 6-8. Privilèges spécifiques de l'objet

Privilège	Actions réalisables par l'utilisateur	Objet
Activer les batteries de serveurs et les pools de postes de travail	Activer et désactiver des pools de postes de travail.	Pool de postes de travail, batterie de serveurs
Autoriser des pools de postes de travail et d'applications	Ajouter et supprimer des autorisations d'utilisateur.	Pool de postes de travail, pool d'applications
Gérer l'image de pool de postes de travail de Composer	Resynchroniser, actualiser et rééquilibrer des pools de clone lié et modifier l'image de pool par défaut.	Pool de postes de travail
Gérer une machine	Effectuer toutes les opérations associées aux machines et aux sessions.	Machine
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
Gérer des batteries de serveurs et des pools de postes de travail et d'applications	Ajouter, modifier et supprimer des batteries de serveurs. Ajouter, modifier, supprimer et autoriser des pools de postes de travail et d'applications. Ajouter et supprimer des machines.	Pool de postes de travail, pool d'applications, batterie de serveurs
Gérer des sessions	Déconnectez et fermez des sessions, et envoyez des messages aux utilisateurs.	Session
Gérer l'opération de redémarrage	Réinitialisez des machines virtuelles ou redémarrez des postes de travail virtuels.	Machine

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 6-9 décrit les privilèges internes et répertorie les rôles prédéfinis qui contiennent chaque privilège.

Tableau 6-9. 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 groupe d'accès racine en plus de l'accès à 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 6-10 répertorie des tâches de gestion des pools communes et montre les privilèges requis pour effectuer chaque tâche.

Tableau 6-10. Privilèges et tâches de gestion des pools

Tâche	Privilèges requis
Activer ou désactiver un pool de postes de travail	**Activer les batteries de serveurs et les pools de postes de travail**
Autoriser ou supprimer l'autorisation d'utilisateurs sur un pool	**Autoriser des pools de postes de travail et d'applications**
Ajouter un pool	**Gérer des batteries de serveurs et des pools de postes de travail et d'applications**
Modifier ou supprimer un pool	**Gérer des batteries de serveurs et des pools de postes de travail et d'applications**
Ajouter ou supprimer des postes de travail d'un pool	**Gérer des batteries de serveurs et des pools de postes de travail et d'applications**
Actualiser, recomposer, rééquilibrer ou modifier l'image de View Composer par défaut	**Gérer l'image de pool de postes de travail de Composer**
Modifier des groupes d'accès	**Gérer des batteries de serveurs et des pools de postes de travail et d'applications** sur les groupes d'accès source et cible.

Privilèges pour la gestion des machines

Un administrateur doit disposer de certains privilèges pour gérer des machines dans View Administrator.

Tableau 6-11 répertorie les tâches de gestion de machines communes et indique les privilèges requis pour effectuer chaque tâche.

Tableau 6-11. Tâches et privilèges de gestion des machines

Tâche	Privilèges requis
Supprimer une machine virtuelle	**Gérer une machine**
Réinitialiser une machine virtuelle	**Gérer l'opération de redémarrage**
Redémarrer un poste de travail virtuel	**Gérer l'opération de redémarrage**
Affecter ou supprimer une propriété d'utilisateur	**Gérer une machine**
Entrer ou quitter le mode de maintenance	**Gérer une machine**
Se déconnecter ou fermer des sessions	**Gérer des sessions**

Privilèges pour la gestion des disques persistants

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

Tableau 6-12 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 6-12. Privilèges et tâches de gestion des disques persistants

Tâche	Privilèges requis
Détacher un disque	**Gérer des disques persistants** sur le disque et **Gérer des batteries de serveurs et des pools de postes de travail et d'applications** sur le pool.
Attacher un disque	**Gérer des disques persistants** sur le disque et **Gérer des batteries de serveurs et des pools de postes de travail et d'applications** sur la machine.
Modifier un disque	**Gérer des disques persistants** sur le disque et **Gérer des batteries de serveurs et des pools de postes de travail et d'applications** sur le pool sélectionné.
Modifier des groupes d'accès	**Gérer des disques persistants** sur les groupes d'accès sources et cibles.
Recréer un poste de travail	**Gérer des disques persistants** sur le disque et **Gérer des batteries de serveurs et des pools de postes de travail et d'applications** sur le dernier pool.
Importer depuis vCenter	**Gérer des disques persistants** sur le dossier et **Gérer le pool** sur le pool.
Supprimer un disque	**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 6-13 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 6-13. Privilèges et tâches de gestion des utilisateurs et des administrateurs

Tâche	Privilèges requis
Mettre à jour des informations utilisateur générales	**Gérer la configuration et les règles générales**
Envoyer des messages aux utilisateurs	**Gérer des sessions distantes** sur la machine.
Ajouter un utilisateur ou un groupe d'administrateurs	**Gérer des rôles et autorisations**

Tableau 6-13. Privilèges et tâches de gestion des utilisateurs et des administrateurs (suite)

Tâche	Privilèges requis
Ajouter, modifier ou supprimer une autorisation d'administrateur	**Gérer des rôles et autorisations**
Ajouter, modifier ou supprimer un rôle d'administrateur	**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 6-14 montre les privilèges requis pour exécuter des tâches d'administration générale et exécuter des utilitaires de ligne de commande.

Tableau 6-14. Privilèges pour des tâches et des commandes d'administration générales

Tâche	Privilèges requis
Ajouter ou supprimer un groupe d'accès	Doit disposer du rôle Administrators sur le groupe d'accès racine.
Gérer des applications ThinApp et des paramètres dans View Administrator	Doit disposer du rôle Administrators sur le groupe d'accès racine.
Installer Horizon Agent sur une machine non gérée, telle qu'un système physique, une machine virtuelle autonome ou un hôte RDS	**Inscrire l'agent**
Voir ou modifier des paramètres de configuration (sauf pour les administrateurs) dans View Administrator	**Gérer la configuration et les règles générales**
Exécutez toutes les commandes PowerShell et les utilitaires de ligne de commande, sauf pour `vdmadmin` et `vdmimport`.	**Interaction directe**
Utiliser les commandes `vdmadmin` et `vdmimport`	Doit disposer du rôle Administrators sur le groupe d'accès racine.
Utiliser la commande `vdmexport`	Doit disposer du rôle Administrateurs ou du rôle Administrateurs (lecture seule) sur le groupe d'accès 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.

- Créez de nouveaux groupes d'utilisateurs dans Active Directory et attribuez des rôles administratifs View à ces groupes. Évitez d'utiliser des groupes intégrés Windows ou d'autres groupes existants qui peuvent contenir des utilisateurs qui n'ont pas besoin de privilèges View ou qui ne devraient pas en disposer.
- Maintenez à un minimum le nombre d'utilisateurs disposant de privilèges administratifs View.
- Comme le rôle Administrateurs détient tous les privilèges, il ne doit pas être utilisé pour une administration courante.
- 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 groupes d'accès pour isoler les postes de travail et batteries de serveurs sensibles. Déléguez l'administration de ces groupes d'accès à un ensemble limité d'utilisateurs.

- Créez des administrateurs séparés qui peuvent modifier des règles générales et des paramètres de configuration View.

Configuration de stratégies dans Horizon Administrator et Active Directory

7

Vous pouvez utiliser Horizon Administrator pour configurer des stratégies pour des sessions clientes. Vous pouvez configurer les paramètres de stratégie de groupe Active Directory afin de contrôler le comportement du Serveur de connexion View, du protocole d'affichage PCoIP et des alarmes de journalisation et de performances de Horizon 7.

Vous pouvez également configurer des paramètres de stratégie de groupe Active Directory afin de contrôler le comportement d'Horizon Agent, d'Horizon Client pour Windows, d'Horizon Persona Management et de certaines fonctionnalités. Pour plus d'informations sur ces paramètres de stratégie, consultez le document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

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 stratégies qui affectent des utilisateurs et des pools de postes de travail spécifiques sont appelées stratégies au niveau des utilisateurs et stratégies au niveau des pools. Les règles qui affectent toutes les sessions et utilisateurs sont appelées règles générales.

Les stratégies au niveau des utilisateurs héritent des paramètres équivalents des stratégies au niveau des pools de postes de travail. De même, les stratégies au niveau des pools de postes de travail héritent des paramètres équivalents des stratégie globales. Un paramètre de stratégie au niveau des pools de postes de travail a priorité sur le paramètre équivalent de stratégie globale. Un paramètre de stratégie au niveau des utilisateurs a priorité sur les paramètres équivalents de stratégie globale et de stratégie au niveau des pools de postes de travail.

Les paramètres de règle de niveau inférieur peuvent être plus ou moins restrictifs que les paramètres de niveau supérieur équivalents. Par exemple, vous pouvez définir une stratégie globale sur **Refuser** et la stratégie au niveau des pools de postes de travail équivalente sur **Autoriser**, ou l'inverse.

Remarque Seules les stratégies globales sont disponibles pour les pools de postes de travail et d'applications RDS. Vous ne pouvez pas définir des stratégies de niveau utilisateur ou des stratégies de niveau pools pour les pools de postes de travail et d'applications RDS.

- Configurer des règles pour des pools de postes de travail page 132

  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 stratégies pour les utilisateurs page 132

  Vous pouvez configurer des règles de niveau utilisateur pour affecter des utilisateurs spécifiques. Les paramètres de stratégie de niveau utilisateur sont toujours prioritaires par rapport aux paramètres de stratégie généraux et de niveau poste de travail équivalents.

- Règles de View page 133

  Vous pouvez configurer des stratégies View pour affecter toutes les sessions clientes, ou vous pouvez les appliquer pour affecter des pools de 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. Reportez-vous à la section « Règles de View », page 133.

Procédure

1 Dans View Administrator, sélectionnez **Règles > Règles générales**.

2 Cliquez sur **Modifier des stratégies** dans le volet **Règles de View**.

3 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. Reportez-vous à la section « Règles de View », page 133.

Procédure

1 Dans View Administrator, sélectionnez **Catalogue > Pools de postes de travail**.

2 Double-cliquez sur l'ID du pool de postes de travail et cliquez sur l'onglet **Règles**.

L'onglet **Règles** montre les paramètres de règle actuels. Lorsqu'un paramètre est hérité de la stratégie générale équivalente, **Hériter** s'affiche dans la colonne **Stratégie de pools de postes de travail**.

3 Cliquez sur **Modifier les stratégies** dans le volet **Règles de View**.

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

Configurer des stratégies pour les utilisateurs

Vous pouvez configurer des règles de niveau utilisateur pour affecter des utilisateurs spécifiques. Les paramètres de stratégie de niveau utilisateur sont toujours prioritaires par rapport aux paramètres de stratégie généraux et de niveau poste de travail équivalents.

Prérequis

Familiarisez-vous avec les descriptions de règles. Reportez-vous à la section « Règles de View », page 133.

Procédure

1 Dans View Administrator, sélectionnez **Catalogue > Pools de postes de travail**.

2 Double-cliquez sur l'ID du pool de postes de travail et cliquez sur l'onglet **Règles**.

L'onglet **Règles** montre les paramètres de règle actuels. Lorsqu'un paramètre est hérité de la stratégie générale équivalente, **Hériter** s'affiche dans la colonne **Stratégie de pools de postes de travail**.

3 Cliquez sur **Remplacements d'utilisateur** et sur **Ajouter un utilisateur**.

4 Pour rechercher un utilisateur, cliquez sur **Ajouter**, saisissez le nom ou la description de l'utilisateur, puis cliquez sur **Rechercher**.

5 Sélectionnez un ou plusieurs utilisateurs dans la liste, cliquez sur **OK**, puis sur **Suivant**.

La boîte de dialogue Add Individual Policy (Ajouter une règle individuelle) apparaît.

6 Configurez les stratégies de View et cliquez sur **Terminer** pour enregistrer vos modifications.

Règles de View

Vous pouvez configurer des stratégies View pour affecter toutes les sessions clientes, ou vous pouvez les appliquer pour affecter des pools de postes de travail ou des utilisateurs spécifiques.

Tableau 7-1 décrit chaque paramètre de stratégie View.

Tableau 7-1. Règles de View

Règle	Description
Redirection multimédia (MMR)	Détermine si MMR est activé pour les systèmes client. MMR est un filtre de Windows Media Foundation qui permet de transférer des données multimédia de codecs spécifiques sur des postes de travail distants 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 **Refuser**. Si les systèmes clients disposent de ressources insuffisantes pour gérer le décodage multimédia local, laissez le paramètre défini sur **Refuser**. Les données de redirection multimédia (MMR) sont envoyées sur le réseau sans cryptage basé sur une application et peuvent contenir des données sensibles, selon le contenu redirigé. Pour garantir que les données ne puissent pas être surveillées sur le réseau, utilisez MMR uniquement sur un réseau sécurisé.
USB Access (Accès USB)	Détermine si des postes de travail distants peuvent utiliser des périphériques USB connectés au système client. La valeur par défaut est **Autoriser**. Pour empêcher l'utilisation de périphériques externes pour des raisons de sécurité, passez le paramètre sur **Refuser**.
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 distant. La valeur par défaut est **Autoriser** avec une priorité **Moyenne**.

Utilisation des fichiers de modèle d'administration de stratégie de groupe Horizon 7

Horizon 7 fournit plusieurs fichiers de modèle d'administration (ADM et ADMX) de stratégie de groupe propres à un composant. Vous pouvez optimiser et sécuriser des applications et des postes de travail distants en ajoutant les paramètres de stratégie de ces fichiers de modèle ADM et ADMX à un nouveau GPO ou à un GPO existant dans Active Directory.

Remarque Dans Horizon 7 version 7.1, les fichiers de modèle d'administration ADM sont obsolètes et les fichiers de modèle d'administration ADMX sont ajoutés.

Tous les fichiers ADMX qui fournissent des paramètres de stratégie de groupe pour Horizon 7 sont disponibles dans un fichier groupé `.zip` nommé `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip`, où *x.x.x* est la version et *yyyyyyy* le numéro de build. Vous pouvez télécharger le fichier sur le site de téléchargement de VMware à l'adresse https://my.vmware.com/web/vmware/downloads. Sous Desktop & End-User Computing, sélectionnez le téléchargement de VMware Horizon 7, qui inclut le fichier groupé `.zip`.

Les fichiers de modèle ADM et ADMX de Horizon 7 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 distants, quelle que soit la personne qui se connecte au poste de travail.
- Les stratégies Configuration d'utilisateur définissent des stratégies qui s'appliquent à tous les utilisateurs, quel que soit l'application ou le poste de travail distant auquel ils se connectent. Les stratégies Configuration d'utilisateur remplacent les stratégies Configuration d'ordinateur équivalentes.

Microsoft Windows applique les stratégies au démarrage du poste de travail et lorsque les utilisateurs se connectent.

Fichiers de modèle d'administration ADMX et ADM d' Horizon 7

Les fichiers de modèle d'administration ADMX et ADM d'Horizon 7 fournissent des paramètres de stratégie de groupe qui vous permettent de contrôler et d'optimiser les composants d'Horizon 7.

Remarque Dans Horizon 7 version 7.1, les fichiers de modèle d'administration ADM sont obsolètes et les fichiers de modèle d'administration ADMX sont ajoutés.

Tableau 7-2. Fichiers de modèle d'administration ADMX et ADM d'Horizon

Nom du modèle	Fichier de modèle	Description
Configuration d'Horizon Agent	`vdm_agent.admx` `vdm_agent.adm`	Contient des paramètres de stratégie liés aux composants d'authentification et d'environnement d'Horizon Agent. Reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.
Configuration d'Horizon Client	`vdm_client.admx` `vdm_client.adm`	Contient des paramètres de stratégie liés à Horizon Client pour Windows. Les clients qui se connectent de l'extérieur du domaine d'hôte du Serveur de connexion ne sont pas affectés par les stratégies appliquées à Horizon Client. Consultez le document *Utilisation de VMware Horizon Client pour Windows*.

Tableau 7-2. Fichiers de modèle d'administration ADMX et ADM d'Horizon (suite)

Nom du modèle	Fichier de modèle	Description
Redirection URL de VMware Horizon	`urlRedirection-enUS.admx` `urlRedirection-enUS.adm`	Contient des paramètres de stratégie liés à la fonctionnalité de redirection de contenu URL. Si vous ajoutez ce modèle à un GPO pour un pool de postes de travail distants ou un pool d'applications, certains liens URL sur lesquels vous cliquez à l'intérieur des applications ou des postes de travail distants peuvent être redirigés vers un client Windows et ouverts dans un navigateur côté client. Si vous ajoutez ce modèle à un GPO côté client, lorsqu'un utilisateur clique sur certains liens URL dans un système client Windows, l'URL peut être ouverte dans une application ou un poste de travail distant. Consultez les documents *Configuration des fonctionnalités de poste de travail distant dans Horizon 7* et *Utilisation de VMware Horizon Client pour Windows*.
Configuration du Serveur de connexion	`vdm_server.admx` `vdm_server.adm`	Contient des paramètres de stratégie liés au Serveur de connexion. Reportez-vous à la section « Paramètres de modèle d'administration ADMX ou ADM pour la configuration du Serveur de connexion Horizon », page 136.
configuration commune de View	`vdm_common.admx` `vdm_common.adm`	Contient des paramètres de stratégie communs à tous les composants Horizon. Reportez-vous à la section « Paramètres de modèle d'administration ADMX et ADM pour la configuration commune d'Horizon 7 », page 137.
variables de session PCoIP	`pcoip.admx` `pcoip.adm`	Contient des paramètres de stratégie liés au protocole d'affichage PCoIP. Reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.
Variables de session de client PCoIP	`pcoip.client.admx` `pcoip.client.adm`	Contient des paramètres de stratégie liés au protocole d'affichage PCoIP qui affectent Horizon Client pour Windows. Consultez le document *Utilisation de VMware Horizon Client pour Windows*.
Configuration d'Horizon Persona Management	`ViewPM.admx` `ViewPM.adm`	Contient des paramètres de stratégie liés à Horizon Persona Management. Reportez-vous au document *Configuration des postes de travail virtuels dans Horizon 7*.
Services Bureau à distance	`vmware_rdsh.admx` `vmware_rdsh.adm`	Contient des paramètres de stratégie liés aux services Bureau à distance. Reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.
Configuration de l'Audio/Vidéo en temps réel	`vdm_agent_rtav.admx` `vdm_agent_rtav.adm`	Contient des paramètres de stratégie liés à des webcams qui sont utilisées avec la fonctionnalité d'Audio/Vidéo en temps réel. Reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

Tableau 7-2. Fichiers de modèle d'administration ADMX et ADM d'Horizon (suite)

Nom du modèle	Fichier de modèle	Description
Redirection de scanner	`vdm_agent_scanner.admx` `vdm_agent_scanner.adm`	Contient des paramètres de stratégie liés à des périphériques d'analyse qui sont redirigés pour une utilisation dans des applications et des postes de travail publiés. Reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.
Redirection de port série	`vdm_agent_serialport.admx` `vdm_agent_serialport.adm`	Contient des paramètres de stratégie liés à des ports série (COM) qui sont redirigés pour une utilisation dans des postes de travail virtuels. Reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

Paramètres de modèle d'administration ADMX ou ADM pour la configuration du Serveur de connexion Horizon

Les fichiers de modèle d'administration ADMX (`vdm_server.admx`) ou ADM (`vdm_server.adm`) pour la configuration de View Server contiennent des paramètres de stratégie liés à tous les Serveurs de connexion Horizon.

Tableau 7-3 décrit chaque paramètre de stratégie dans le fichier de modèle d'administration ADMX ou ADM pour la configuration du Serveur de connexion. Le modèle ne contient que des paramètres de Configuration d'ordinateur. Tous les paramètres se trouvent dans le dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Configuration de VMware View Server** dans l'Éditeur de gestion des stratégies de groupe.

Remarque Dans Horizon 7 version 7.1, les fichiers de modèle d'administration ADM sont obsolètes et les fichiers de modèle d'administration ADMX sont ajoutés.

Tableau 7-3. Paramètres de modèle pour la configuration d'Horizon Server

Paramètre	Propriétés
`Enumerate Forest Trust Child Domains`	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 de manière récursive jusqu'à ce que tous les domaines approuvés soient détectés. Ces informations sont transmises au Serveur de connexion pour s'assurer que le client dispose de tous les domaines approuvés lors des ouvertures de session. Cette propriété est activée par défaut. Lorsqu'elle est désactivée, seuls les domaines approuvés directement sont énumérés et la connexion aux contrôleurs de domaine distants n'est pas assurée. **Remarque** Dans des environnements contenant des relations de domaine complexes (telles que celles utilisant plusieurs structures de forêt avec approbations entre domaines de leurs forêts), le processus peut prendre plusieurs minutes.
`Recursive Enumeration of Trusted Domains`	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 au Serveur de connexion View 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.
`Windows Password Authentication Mode`	Sélectionnez le mode d'authentification de mot de passe Windows. ■ `KerberosOnly`. Authentifiez-vous avec Kerberos. ■ `KerberosWithFallbackToNTLM`. Authentifiez-vous avec Kerberos, mais revenez à l'utilisation de NTLM en cas d'échec. ■ `Legacy`. Authentifiez-vous avec NTLM, mais revenez à l'utilisation de Kerberos en cas d'échec. Utilisé pour prendre en charge les contrôleurs de domaine NT hérités. La valeur par défaut est `KerberosOnly`.

Paramètres de modèle d'administration ADMX et ADM pour la configuration commune d' Horizon 7

Les fichiers de modèle d'administration ADMX (`vdm_common.admx`) et ADM (`vdm_common.adm`) pour la configuration commune d'Horizon 7 contiennent des paramètres de stratégie communs à tous les composants Horizon. Ces modèles ne contiennent que des paramètres de Configuration d'ordinateur. Dans Horizon 7 version 7.1, les fichiers de modèle d'administration ADM sont obsolètes et les fichiers de modèle d'administration ADMX sont ajoutés.

paramètres de configuration de journal

Tableau 7-4 décrit chaque paramètre de stratégie pour la configuration de journal dans les fichiers de modèle d'administration ADMX et ADM pour la configuration commune d'Horizon. Tous les paramètres se trouvent dans le dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Configuration commune de VMware View > Configuration de journal** dans l'Éditeur de gestion des stratégies de groupe.

Tableau 7-4. Modèle de configuration commune de View : paramètres de configuration de journal

Paramètre	Propriétés
`Number of days to keep production logs`	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`	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`	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`	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.
`Send logs to a Syslog server`	Permet l'envoi de journaux de View Server à un serveur Syslog tel que VMware vCenter Log Insight. Les journaux sont envoyés par tous les serveurs View Server de l'unité d'organisation (UO) ou du domaine dans lequel cet objet de stratégie de groupe (objet GPO) est configuré. Vous pouvez envoyer les journaux d'Horizon Agent à un serveur Syslog en activant ce paramètre dans un objet GPO qui est lié à une UO contenant vos postes de travail. Pour envoyer des données de journaux à un serveur Syslog, activez ce paramètre et spécifiez le niveau de journal et le nom de domaine complet ou l'adresse IP du serveur. Vous pouvez spécifier un autre port si vous ne souhaitez pas utiliser le port par défaut 514. Séparez chaque élément de votre spécification par une barre verticale (`|`). Utilisez la syntaxe suivante : `Niveau de journal|FQDN ou IP du serveur [|Numéro de port(514 par défaut)]` Par exemple : `Debug|192.0.2.2` **Important** Les données Syslog sont envoyées sur le réseau sans chiffrement logiciel. Comme les journaux de View Server peuvent contenir des données sensibles, évitez d'envoyer des données Syslog sur un réseau non sécurisé. Si possible, utilisez une sécurité de couche de liaison telle qu'IPsec pour éliminer toute possibilité de surveillance de ces données sur le réseau.

paramètres d'alarme de performance

Tableau 7-5 décrit les paramètres d'alarme de performance dans les fichiers de modèle d'administration ADMX et ADM pour la configuration commune d'Horizon. Tous les paramètres se trouvent dans le dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Configuration commune de VMware View > Alarmes de performance** dans l'Éditeur de gestion des stratégies de groupe.

Tableau 7-5. Modèle de configuration commune de View : paramètres d'alarme de performance

Paramètre	Propriétés
`CPU and Memory Sampling Interval in Seconds`	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`	Spécifie le seuil auquel l'utilisation du CPU global du système est journalisée. Lorsque plusieurs processeurs sont disponibles, ce pourcentage représente l'utilisation combinée.

Tableau 7-5. Modèle de configuration commune de View : paramètres d'alarme de performance (suite)

Paramètre	Propriétés
`Overall memory usage percentage to issue log info`	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`	Spécifie le seuil auquel l'utilisation de CPU d'un processus individuel est journalisée.
`Process memory usage percentage to issue log info`	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`	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 Serveur de connexion Horizon et Horizon Agent. Ils ne s'appliquent pas aux systèmes Horizon Client.

Paramètres de sécurité

Tableau 7-6 décrit les paramètres de sécurité dans les fichiers de modèle d'administration ADMX et ADM pour la configuration commune d'Horizon. Tous les paramètres se trouvent dans le dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Configuration commune de VMware View > Paramètres de sécurité** dans l'Éditeur de gestion des stratégies de groupe.

Tableau 7-6. Modèle de configuration commune de View : paramètres de sécurité

Paramètre	Propriétés
`Only use cached revocation URLS`	La vérification de la révocation des certificats n'a accès qu'aux URL mises en cache. Si ce paramètre n'est pas configuré, la valeur par défaut est définie sur false.
`Revocation URL check timeout milliseconds`	Délai d'expiration cumulatif sur toutes les récupérations d'URL de révocation en millisecondes. Une absence de configuration ou une valeur définie sur 0 signifie que la gestion par défaut de Microsoft est utilisée.
`Type of certificate revocation check`	Sélectionnez le type de vérification de la révocation des certificats à effectuer : ■ aucune ■ EndCertificateOnly ■ WholeChain ■ WholeChain La valeur par défaut est WholeChainButRoot.

Paramètres généraux

Tableau 7-7 décrit les paramètres généraux dans les fichiers de modèle d'administration ADMX et ADM pour la configuration commune d'Horizon. Tous les paramètres se trouvent dans le dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Configuration commune de VMware View** dans l'Éditeur de gestion des stratégies de groupe.

Tableau 7-7. Modèle de configuration commune de View : paramètres généraux

Paramètre	Propriétés
`Disk threshold for log and events in Megabytes`	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`	Détermine si les événements de suivi et de débogage sont inclus dans les fichiers journaux.
`Override the default View Windows event generation`	Les valeurs suivantes sont prises en charge : ■ 0 = Des entrées de journal des événements ne sont produites que pour des événements d'affichage (aucune entrée de journal des événements n'est générée pour les messages de journal) ■ 1 = Des entrées de journal des événements sont produites en mode de compatibilité 4.5 (et antérieur). Des entrées de journal des événements ne sont pas produites pour les événements d'affichage standard. Les entrées de journal des événements sont basées uniquement sur le texte du fichier journal. ■ 2 = Des entrées de journal des événements sont produites en mode de compatibilité 4.5 (et antérieur) avec des événements d'affichage également inclus.

Maintenance des composants View 8

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 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 et les fichiers de base de données View Composer sauvegardés.

Vous pouvez utiliser les fonctionnalités de sauvegarde et de restauration pour conserver et migrer des données de configuration de View.

Sauvegarde des données du Serveur de connexion View et de View Composer

Après avoir terminé la configuration initiale du Serveur de connexion View, vous devez planifier des sauvegardes régulières de vos données de configuration de View et de View Composer. Vous pouvez conserver vos données View et View Composer en utilisant View Administrator.

View stocke des données de configuration du 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 sauvegarde les données de configuration de 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 obtenir une description de View LDAP, reportez-vous à la section « Répertoire View LDAP », page 46

Vous pouvez effectuer les sauvegardes de plusieurs façons.

- Planifiez des sauvegardes automatiques en utilisant la fonctionnalité Sauvegarde de configuration de View.
- 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 le Serveur de connexion View », page 143.

Les recommandations suivantes s'appliquent à la sauvegarde des données de configuration de View :

- View peut exporter des données de configuration de n'importe quelle instance du Serveur de connexion View.
- Si vous possédez plusieurs instances du 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 du Serveur de connexion View agissent comme votre mécanisme de sauvegarde. Lorsque View synchronise des données dans des instances répliquées du Serveur de connexion View, toutes les données perdues dans une instance peuvent être perdues dans tous les membres du groupe.
- Si le Serveur de connexion View utilise plusieurs instances de vCenter Server avec plusieurs services View Composer, View sauvegarde toutes les bases de données View Composer associées aux instances de vCenter Server.

Planifier des sauvegardes de configuration de View

Vous pouvez planifier la sauvegarde de vos données de configuration de View à intervalles réguliers. View sauvegarde le contenu du référentiel View LDAP dans lequel vos instances du Serveur de connexion View stockent leurs données de configuration.

Vous pouvez sauvegarder la configuration immédiatement en sélectionnant l'instance du 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 d'View », page 143.

Procédure

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

2 Dans l'onglet **Serveurs de connexion**, sélectionnez l'instance du Serveur de connexion View à sauvegarder et cliquez sur **Modifier**.

3 Dans l'onglet **Sauvegarder**, spécifiez les paramètres de sauvegarde de configuration de View pour configurer la fréquence de sauvegarde, le nombre maximal de sauvegardes et l'emplacement du dossier des fichiers de sauvegarde.

4 (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**.

5 Cliquez sur **OK**.

Paramètres de sauvegarde de configuration d' View

View peut sauvegarder vos données de configuration du Serveur de connexion View et de View Composer à intervalles réguliers. Dans View Administrator, vous pouvez définir la fréquence et d'autres aspects des opérations de sauvegarde.

Tableau 8-1. Paramètres de sauvegarde de configuration d' View

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 du Serveur de connexion View. Le nombre doit être un entier supérieur à 0. Lorsque le nombre maximal est atteint, View supprime le fichier de sauvegarde le plus ancien. Ce paramètre s'applique également aux fichiers de sauvegarde créés lorsque vous utilisez la fonction **Sauvegarder maintenant**.
Emplacement de dossier	Emplacement par défaut des fichiers de sauvegarde sur l'ordinateur sur lequel le Serveur de connexion View est en cours d'exécution : `C:\Programdata\VMWare\VDM\backups` Lorsque vous utilisez l'option **Sauvegarder maintenant**, View stocke également les fichiers de sauvegarde à cet emplacement.

Exporter des données de configuration depuis le Serveur de connexion View

Vous pouvez sauvegarder des données de configuration d'une instance du 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 du Serveur de connexion View. Si vous possédez plusieurs instances du 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 du Serveur de connexion View en tant qu'utilisateur dans le rôle Administrators (Administrateurs) ou Administrators (Read only) (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`, reportez-vous au document *Intégration de 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 « Restauration des données de configuration de Serveur de connexion View et View Composer », page 145

Restauration des données de configuration de Serveur de connexion View et View Composer

Vous pouvez restaurer manuellement les fichiers de configuration LDAP du Serveur de connexion View et les fichiers de base de données View Composer qui ont été sauvegardés par View.

Vous exécutez manuellement des utilitaires séparés pour restaurer les données de configuration du Serveur de connexion View et de 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 du Serveur de connexion View et de View Composer », page 141.

Vous utilisez l'utilitaire `vdmimport` pour importer les données du Serveur de connexion View des fichiers de sauvegarde LDIF vers le référentiel View LDAP dans l'instance du 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 certains cas, il peut s'avérer nécessaire d'installer la version actuelle d'une instance du Serveur de connexion View et de restaurer la configuration existante de View en important les fichiers de configuration LDAP du Serveur de connexion View. Vous pouvez avoir besoin de cette procédure dans le cadre d'un plan de continuité de l'activité et de récupération d'urgence pour configurer un deuxième centre de données avec la configuration existante de View ou pour d'autres raisons. Pour plus d'informations, reportez-vous à la section « Réinstaller le Serveur de connexion View avec une configuration de sauvegarde » dans le document *Installation de View*.

Importer des données de configuration dans le Serveur de connexion View

Vous pouvez restaurer des données de configuration d'une instance du 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 du 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 du Serveur de connexion View et de View Composer », page 141

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
  ```

- Connectez-vous à une instance du Serveur de connexion View en tant qu'utilisateur disposant du rôle Administrateurs.

- 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 Arrêtez toutes les instances of View Composer en arrêtant le service Windows VMware Horizon View Composer sur les serveurs sur lesquels View Composer s'exécute.

2 Arrêtez toutes les instances du serveur de sécurité en arrêtant le service Windows Serveur de sécurité VMware Horizon sur tous les serveurs de sécurité.

3 Désinstallez toutes les instances du Serveur de connexion View.

Désinstallez Serveur de connexion VMware Horizon View et l'instance d'AD LDS Instance VMwareVDMDS.

4 Installez une instance du Serveur de connexion View.

5 Arrêtez l'instance du Serveur de connexion View en arrêtant le service Windows Serveur de connexion VMware Horizon.

6 Cliquez sur **Démarrer > Invite de commande**.

7 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.

8 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
```

9 Désinstallez le Serveur de connexion View.

Désinstallez uniquement le module Serveur de connexion VMware Horizon View.

10 Réinstallez Serveur de connexion View.

11 Connectez-vous à View Administrator et vérifiez que la configuration est correcte.

12 Démarrez les instances de View Composer.

13 Réinstallez les instances du serveur réplica.

14 Démarrez les instances du serveur de sécurité.

Si la configuration des serveurs de sécurité risque d'être incohérente, ils doivent également être désinstallés plutôt qu'arrêtés, puis réinstallés à la fin du processus.

La commande `vdmimport` met à jour le référentiel View LDAP dans le Serveur de connexion View avec les données de configuration du fichier LDIF. Pour plus d'informations sur la commande `vdmimport`, reportez-vous au document *Intégration de View*.

Remarque Assurez-vous que la configuration qui est restaurée correspond aux machines virtuelles qui sont connues de vCenter Server et de View Composer, s'il est utilisé. Si nécessaire, restaurez la configuration de View Composer à partir d'une sauvegarde. Reportez-vous à la section « Restaurer une base de données View Composer », page 147. Après la restauration de la configuration de View Composer, vous devrez peut-être résoudre manuellement des incohérences si les machines virtuelles dans vCenter Server ont changé depuis la sauvegarde de la configuration de View Composer.

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 View Composer expérimentés 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 stocke les fichiers de sauvegarde sur le lecteur `C:` de l'ordinateur Serveur de connexion View, dans le répertoire `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 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.
- `BackupFilePath` : chemin d'accès au fichier de sauvegarde View Composer.

Les paramètres `DsnName` et `BackupFilePath` sont requis et ne peuvent pas être des chaînes vides. Les paramètres `Username` et `Password` sont facultatifs.

Procédure

1. Copiez les fichiers de sauvegarde View Composer de l'ordinateur Serveur de connexion View vers un emplacement qui est accessible à l'ordinateur sur lequel le service VMware Horizon View Composer est installé.
2. Sur l'ordinateur sur lequel View Composer est installé, arrêtez le service VMware Horizon View Composer.

3 Ouvrez une invite de commande Windows et accédez au fichier exécutable `SviConfig`.

Le fichier est situé avec l'application View Composer. Le chemin d'accès par défaut est `C:\Program Files (x86)\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 (x86)\VMware\VMware View
Composer\Backup–20090304000010–foobar_test_org.SVI"
```

5 Démarrez le service VMware Horizon View Composer.

Suivant

Pour voir les codes de résultat de la sortie `SviConfig restoredata`, reportez-vous à la section « Codes de résultat pour la restauration de la base de données View Composer », page 148.

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 8-2. 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 VMware Horizon 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 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 Horizon View Composer.

2 Ouvrez une invite de commande Windows et accédez au fichier exécutable `SviConfig`.

Le fichier est situé avec l'application View Composer.

`View-Composer-installation-directory``\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 149.

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 8-3. 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 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 du Serveur de connexion View, 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 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 **Tableau de bord**.

2 Dans le volet Intégrité du système, développez **Composants View**, **Composants vSphere** ou **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.

Suivant

Utilisez vCenter Server pour surveiller les clusters Virtual SAN et les disques qui participent à une banque de données Virtual SAN. Pour obtenir plus d'informations sur la surveillance de Virtual SAN dans vSphere 5.5 Update 1, reportez-vous au document *Stockage de vSphere* et au document *Surveillance et performance de vSphere*. Pour plus d'informations sur la surveillance de Virtual SAN dans vSphere 6 ou version ultérieure, reportez-vous au document *Administration de VMware Virtual SAN*.

Surveiller l'état des machines

Vous pouvez rapidement contrôler l'état des machines de votre déploiement de View dans le tableau de bord de View Administrator. Par exemple, vous pouvez afficher toutes les machines déconnectées ou les machines qui sont en mode de maintenance.

Prérequis

Familiarisez-vous avec les valeurs d'état des machines virtuelles. Reportez-vous à la section « État des machines virtuelles vCenter Server », page 208.

Procédure

1 Dans View Administrator, cliquez sur **Tableau de bord**.

2 Dans le volet État des machines, développez un dossier d'état.

Option	Description
Préparation	Répertorie les états lorsque la machine est en cours de provisionnement, de suppression ou en mode de maintenance.
Machines problématiques	Répertorie les états d'erreur.
Préparé pour l''utilisation	Répertorie les états lorsque la machine est prête à être utilisée.

3 Recherchez l'état des machines et cliquez sur le nombre affiché sous forme de lien hypertexte situé en regard.

La page **Machines** affiche toutes les machines se trouvant dans l'état sélectionné.

Suivant

Vous pouvez cliquer sur un nom de machine pour voir des détails sur cette dernière ou cliquer sur la flèche Précédent dans View Administrator pour revenir à la page Tableau de bord.

Présentation des services View

Le fonctionnement d'instances du 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 Services Microsoft Windows pour arrêter ou démarrer les services View. Si vous arrêtez les services View sur un hôte du Serveur de connexion View ou sur un serveur de sécurité, les utilisateurs finaux ne pourront pas se connecter à leurs applications ou postes de travail distants tant que vous ne les aurez pas redémarrés. Vous pouvez également avoir besoin de redémarrer un service qui a cessé de fonctionner ou si la fonctionnalité de View qu'il contrôle ne répond plus.

Arrêter et démarrer les services View

Le fonctionnement d'instances du Serveur de connexion View et de serveurs de sécurité dépend de plusieurs services qui s'exécutent sur le système. Il est parfois nécessaire d'arrêter et de démarrer ces services manuellement lors du dépannage de dysfonctionnements de View.

Lorsque vous arrêtez les services View, les utilisateurs finaux ne peuvent pas se connecter à leurs applications et à leurs postes de travail distants. Vous devez effectuer cet arrêt à une heure déjà planifiée pour la maintenance du système ou avertir les utilisateurs finaux que leur poste de travail et leurs applications seront temporairement indisponibles.

Remarque Arrêtez uniquement le service Serveur de connexion VMware Horizon View sur un hôte du Serveur de connexion View ou le service Serveur de sécurité VMware Horizon View sur un serveur de sécurité. N'arrêtez pas d'autres services de composant.

Prérequis

Familiarisez-vous avec les services exécutés sur les hôtes du Serveur de connexion View et les serveurs de sécurité comme expliqué dans les sections « Services sur un hôte du Serveur de connexion View », page 152 et « Services sur un serveur de sécurité », page 152.

Procédure

1 Démarrez l'outil Windows Services en saisissant **`services.msc`** à l'invite de commande.

2 Sélectionnez le service Serveur de connexion VMware Horizon View sur un hôte du Serveur de connexion View ou le service Serveur de sécurité VMware View sur un serveur de sécurité, et cliquez sur **Arrêter**, **Redémarrer** ou **Démarrer**, selon le cas.

3 Vérifiez que l'état du service répertorié change comme prévu.

Services sur un hôte du Serveur de connexion View

Le fonctionnement de View dépend de plusieurs services s'exécutant sur un hôte du Serveur de connexion View.

Tableau 8-4. Services d'un hôte du Serveur de connexion View

Nom du service	Type de démarrage	Description
VMware Horizon View Blast Secure Gateway	Automatique	Fournit des services HTML Access et Blast Extreme sécurisés. Ce service doit être en cours d'exécution si des clients se connectent au Serveur de connexion View via Blast Secure Gateway.
Serveur de connexion VMware Horizon View	Automatique	Fournit des services de Broker pour les connexions. Ce service doit toujours être en cours d'exécution. 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 ni n'arrête le service VMwareVDMDS ou VMware Horizon View Script Host.
Composant de VMware Horizon View Framework	Manuel	Fournit des services de journalisation des événements, de sécurité et d'infrastructure COM+. Ce service doit toujours être en cours d'exécution.
Composant du bus de message VMware Horizon View	Manuel	Fournit des services de messagerie entre les composants View. Ce service doit toujours être en cours d'exécution.
VMware Horizon View PCoIP Secure Gateway	Manuel	Fournit des services PCoIP Secure Gateway. Ce service doit être en cours d'exécution si des clients se connectent au Serveur de connexion View via PCoIP Secure Gateway.
Hôte de script VMware Horizon View	Désactivé	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.
Composant VMware Horizon View Security Gateway	Manuel	Fournit des services de passerelle communs. Ce service doit toujours être en cours d'exécution.
Composant Web VMware Horizon View	Manuel	Fournit des services Web. Ce service doit toujours être en cours d'exécution.
VMwareVDMDS	Automatique	Fournit des services d'annuaire LDAP. Ce service doit toujours être en cours d'exécution. Pendant les mises à niveau de View, ce service garantit la migration correcte des données existantes.

Services sur un serveur de sécurité

Le fonctionnement de View dépend de plusieurs services s'exécutant sur un serveur de sécurité.

Tableau 8-5. Services de serveur de sécurité

Nom du service	Type de démarrage	Description
VMware Horizon View Blast Secure Gateway	Automatique	Fournit des services HTML Access et Blast Extreme sécurisés. Ce service doit être en cours d'exécution si des clients se connectent à ce serveur de sécurité via Blast Secure Gateway.
Serveur de sécurité VMware Horizon View	Automatique	Fournit des services de serveur de sécurité. Ce service doit toujours être en cours d'exécution. Si vous démarrez ou arrêtez ce service, il démarre ou arrête également les services Framework et Security Gateway.

Tableau 8-5. Services de serveur de sécurité (suite)

Nom du service	Type de démarrage	Description
Composant de VMware Horizon View Framework	Manuel	Fournit des services de journalisation des événements, de sécurité et d'infrastructure COM+. Ce service doit toujours être en cours d'exécution.
VMware Horizon 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 ce serveur de sécurité via PCoIP Secure Gateway.
Composant VMware Horizon View Security Gateway	Manuel	Fournit des services de passerelle communs. Ce service doit toujours être en cours d'exécution.

Modifier la clé de licence produit

Si la licence d'un système expire ou si vous souhaitez accéder à des fonctionnalités de View qui ne sont pas actuellement sous licence, utilisez View Administrator pour modifier la clé de licence produit.

Vous pouvez ajouter une licence à View pendant l'exécution de View. Vous n'avez pas à redémarrer le système, et l'accès aux postes de travail et aux applications n'est pas interrompu.

Prérequis

Pour que View et des fonctionnalités complémentaires telles que View Composer et des applications distantes fonctionnent correctement, obtenez une clé de licence produit valide.

Procédure

1 Dans View Administrator, sélectionnez **Configuration de View > Licence produit et utilisation**.

Les cinq premiers et les cinq derniers caractères de la clé de licence actuelle sont affichés dans le volet **Licence**.

2 Cliquez sur **Modifier la licence**.

3 Saisissez le numéro de série de licence et cliquez sur **OK**.

La fenêtre Licence produit affiche les informations de licence mises à jour.

4 Vérifiez la date d'expiration de la licence.

5 Vérifiez que les licences d'utilisation à distance des postes de travail et des applications, et de View Composer sont activées ou désactivées en fonction de l'édition de VMware Horizon 7 que la licence produit vous autorise à utiliser.

Les fonctionnalités et capacités de VMware Horizon 7 ne sont pas toutes disponibles dans toutes les éditions. Pour comparer les fonctionnalités de chaque édition, consultez http://www.vmware.com/files/pdf/products/horizon-view/VMware-Horizon-View-Pricing-Licensing-FAQ.pdf.

6 Vérifiez que le modèle d'utilisation de licence correspond au modèle utilisé dans votre licence produit.

L'utilisation est comptée selon le nombre d'utilisateurs nommés ou d'utilisateurs simultanés, en fonction de l'édition et des conditions d'utilisation de votre licence produit.

Surveillance de l'utilisation des licences produit

Dans View Administrator, vous pouvez surveiller les utilisateurs actifs connectés simultanément à View. La page **Licence produit et utilisation** affiche le nombre d'utilisations actuel et le nombre d'utilisations maximal historique. Vous pouvez utiliser ces chiffres pour effectuer le suivi de l'utilisation de votre licence produit. Vous pouvez également réinitialiser les données utilisateur historiques et recommencer avec les données actuelles.

View fournit deux modèles d'utilisation de licences, un pour les utilisateurs nommés et l'autre pour les utilisateurs simultanés. View compte les utilisateurs nommés et les utilisateurs simultanés dans votre environnement, quelles que soient l'édition ou les conditions d'utilisation de modèle de votre licence produit.

Pour les utilisateurs nommés, View compte le nombre d'utilisateurs uniques qui ont accédé à l'environnement View. Si un utilisateur nommé exécute plusieurs postes de travail mono-utilisateur, des postes de travail RDS et des applications distantes, l'utilisateur est compté une fois.

Pour les utilisateurs nommés, la colonne **Actuel** de la page **Licence produit et utilisation** affiche le nombre d'utilisateurs depuis la première configuration de votre déploiement de View ou depuis la dernière réinitialisation du **Nombre d'utilisateurs nommés**. La colonne **Maximum** ne s'applique pas aux utilisateurs nommés.

Pour les utilisateurs simultanés, View compte les connexions de poste de travail mono-utilisateur par session. Si un utilisateur simultané exécute plusieurs postes de travail mono-utilisateur, chaque session de poste de travail connectée est comptée séparément.

Pour les utilisateurs simultanés, les connexions d'application et de poste de travail RDS sont comptées par utilisateur. Si un utilisateur simultané exécute plusieurs sessions de poste de travail RDS et plusieurs applications, l'utilisateur n'est compté qu'une fois, même si différents postes de travail ou applications RDS sont hébergés sur différents hôtes RDS. Si un utilisateur simultané exécute un poste de travail mono-utilisateur et des postes de travail et applications RDS supplémentaires, l'utilisateur n'est compté qu'une fois.

Pour les utilisateurs simultanés, la colonne **Maximum** de la page **Licence produit et utilisation** affiche le nombre maximal de sessions de poste de travail simultanées et d'utilisateurs de postes de travail et d'applications RDS depuis la première configuration de votre déploiement de View ou depuis la dernière réinitialisation du **Nombre maximal**.

Réinitialiser les données d'utilisation des licences produit

Dans View Administrator, vous pouvez réinitialiser les données d'utilisation historiques des produits et recommencer avec les données actuelles.

Un administrateur avec le privilège **Gérer la configuration et les règles générales** peut sélectionner les paramètres **Réinitialiser le nombre maximal** et **Réinitialiser le nombre d'utilisateurs nommés**. Pour limiter l'accès à ces paramètres, n'accordez ce privilège qu'à des administrateurs désignés.

Prérequis

Familiarisez-vous avec l'utilisation des licences produit. Reportez-vous à la section « Surveillance de l'utilisation des licences produit », page 154.

Procédure

1 Dans View Administrator, sélectionnez **Configuration de View > Licence produit et utilisation**.

2 (Facultatif) Dans le volet **Utilisation**, sélectionnez **Réinitialiser le nombre maximal**.

Le nombre maximal historique de connections simultanées est réinitialisé au nombre actuel.

3 (Facultatif) Dans le volet **Utilisation**, sélectionnez **Réinitialiser le nombre d'utilisateurs nommés**.

Le nombre maximal historique d'utilisateurs nommés est réinitialisé à 0.

Remarque La sélection de **Mettre à jour des informations utilisateur générales** sur la page **Utilisateurs et groupes** réinitialise également le nombre maximal historique d'utilisateurs nommés à 0.

Mettre à jour des informations utilisateur générales depuis Active Directory

Vous pouvez mettre à jour View avec les informations actuelles de l'utilisateur stockées dans Active Directory. Cette fonctionnalité 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 fonctionnalité si vous modifiez la liste des domaines externes approuvés dans Active Directory, en particulier si les relations d'approbation modifiées entre des domaines affectent des autorisations utilisateur dans View.

Cette fonctionnalité analyse Active Directory à la recherche des informations utilisateur les plus récentes et actualise la configuration de View.

La mise à jour des informations utilisateur générales réinitialise également le nombre d'utilisateurs nommés à 0. Ce nombre apparaît sur la page **Licence produit et utilisation** dans View Administrator. Reportez-vous à la section « Réinitialiser les données d'utilisation des licences produit », page 154.

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 289.

Prérequis

Vérifiez que vous pouvez vous connecter à View Administrator en tant qu'administrateur disposant du privilège **Gérer la configuration et les règles générales**.

Procédure

1 Dans View Administrator, cliquez sur **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 **Mettre à jour des 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 **Mettre à jour des informations utilisateur générales**.

Migrer View Composer vers une autre machine

Dans certains cas, il peut être nécessaire de migrer un service VMware Horizon View Composer vers une nouvelle machine virtuelle ou physique 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. En outre, il est inutile d'installer View Composer et vCenter Server sur la même machine Windows Server.

Vous pouvez migrer View Composer depuis la machine vCenter Server vers une machine autonome ou depuis une machine autonome vers la machine vCenter Server.

Conseils sur la migration de View Composer

Les étapes requises pour migrer le service VMware Horizon View Composer varient selon que vous souhaitez ou non conserver les machines virtuelles de clone lié existantes.

Pour conserver les machines virtuelles de clone lié dans votre déploiement, le service VMware Horizon View Composer que vous installez sur la nouvelle machine virtuelle ou physique doit continuer à utiliser la base de données View Composer existante. La base de données View Composer contient les données requises pour créer, approvisionner, maintenir et supprimer les clones liés.

Lorsque vous migrez le service VMware Horizon View Composer, vous pouvez également migrer la base de données View Composer vers une nouvelle machine.

Que vous procédiez ou non à la migration de la base de données View Composer, la base de donnée doit être configurée sur une machine disponible dans le même domaine que la nouvelle machine sur laquelle vous installez le service VMware Horizon View Composer ou sur un domaine approuvé.

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 VMware Horizon View Composer, vous devez migrer le conteneur de clés RSA créé par le service VMware Horizon View Composer d'origine. Vous devez importer le conteneur de clés RSA sur la machine sur laquelle vous installez le nouveau service.

Si le service VMware Horizon View Composer actuel ne gère pas de machines virtuelles de clone lié, vous pouvez migrer le service sans utiliser la base de données View Composer existante. Il n'est pas nécessaire de migrer les clés RSA, que vous utilisiez ou non la base de données existante.

Remarque Chaque instance du service VMware Horizon View Composer doit posséder sa propre base de données View Composer. Plusieurs services VMware Horizon 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 une autre machine physique ou virtuelle, si vous prévoyez de conserver vos machines virtuelles de clone lié actuelles, le nouveau service VMware Horizon 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'une machine vCenter Server vers une machine autonome
- D'une machine autonome vers une machine vCenter Server
- D'une machine autonome vers une autre machine autonome
- D'une machine vCenter Server vers une autre machine vCenter Server

Lorsque vous migrez le service VMware Horizon 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 une machine vCenter Server que vous migrez également.

Lorsque vous installez le service VMware Horizon View Composer sur la nouvelle machine, 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 « Conseils sur la migration de View Composer », page 156.
- Familiarisez-vous avec les étapes de migration du conteneur de clés RSA vers le nouveau service VMware Horizon View Composer. Reportez-vous aux sections « Préparer Microsoft .NET Framework pour la migration de clés RSA », page 159 et « Migrer le conteneur de clés RSA vers le nouveau service View Composer », page 160.
- Familiarisez-vous avec l'installation du service VMware Horizon View Composer. Consultez la section « Installation de View Composer » dans le document *Installation de View*.
- Familiarisez-vous avec la configuration d'un certificat SSL pour View Composer. Consultez « Configuration de certificats SSL pour des serveurs View Server » dans le document *Installation de 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 20.

Procédure

1. Désactivez le provisionnement de machine virtuelle dans l'instance de vCenter Server associée au service VMware Horizon View Composer.
   a. Dans View Administrator, sélectionnez **Configuration de View > Serveurs**.
   b. Dans l'onglet **Serveurs 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 VMware Horizon View Composer de la machine actuelle.
4. (Facultatif) Migrez le conteneur de clés RSA vers la nouvelle machine.

5 Installez le service VMware Horizon View Composer sur la nouvelle machine.

Lors de l'installation, spécifiez le nom DSN de la base de données qui était utilisée par le service VMware Horizon 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 VMware Horizon 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 la nouvelle machine.

Vous pouvez copier le certificat qui a été installé pour View Composer sur la machine d'origine ou installer un nouveau certificat.

7 Dans View Administrator, configurez les nouveaux paramètres de View Composer.

a Dans View Administrator, sélectionnez **Configuration de View > Serveurs**.

b Dans l'onglet **vCenter Servers**, sélectionnez l'instance de vCenter Server associée à ce service View Composer et cliquez sur **Modifier**.

c Dans le volet Paramètres de View Composer Server, cliquez sur **Modifier** et fournissez les nouveaux paramètres de View Composer.

Si vous installez View Composer avec vCenter Server sur la nouvelle machine, sélectionnez **View Composer est co-installé avec vCenter Server**.

Si vous installez View Composer sur une machine autonome, sélectionnez **Serveur View Composer Server autonome** et fournissez le FQDN de la machine 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**.

Migrer View Composer sans machines virtuelles de clone lié

Si le service VMware Horizon View Composer actuel ne gère aucune machine virtuelle de clone lié, vous pouvez migrer View Composer vers une nouvelle machine physique ou virtuelle sans migrer les clés RSA vers la nouvelle machine. Le service VMware Horizon 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 VMware Horizon View Composer. Consultez la section « Installation de View Composer » dans le document *Installation de View*.
- Familiarisez-vous avec la configuration d'un certificat SSL pour View Composer. Consultez « Configuration de certificats SSL pour des serveurs View Server » dans le document *Installation de View*.
- Familiarisez-vous avec les étapes de suppression de View Composer de View Administrator. Reportez-vous à la section « Supprimer View Composer de View », page 27.

  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 20.

Procédure

1 Dans View Administrator, supprimez View Composer de View Administrator.

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

   b Dans l'onglet **vCenter Servers**, sélectionnez l'instance de vCenter Server associée au service View Composer et cliquez sur **Modifier**.

   c Dans le volet Paramètres de View Composer Server, cliquez sur **Modifier**.

   d Sélectionnez **Ne pas utiliser View Composer** et cliquez sur **OK**.

2 Désinstallez le service VMware Horizon View Composer de la machine actuelle.

3 Installez le service VMware Horizon View Composer sur la nouvelle machine.

   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 la nouvelle machine.

   Vous pouvez copier le certificat qui a été installé pour View Composer sur la machine d'origine ou installer un nouveau certificat.

5 Dans View Administrator, configurez les nouveaux paramètres de View Composer.

   a Dans View Administrator, sélectionnez **Configuration de View > Serveurs**.

   b Dans l'onglet **vCenter Servers**, sélectionnez l'instance de vCenter Server associée à ce service View Composer et cliquez sur **Modifier**.

   c Dans le volet Paramètres de View Composer Server, cliquez sur **Modifier**.

   d Fournissez les nouveaux paramètres de View Composer.

      Si vous installez View Composer avec vCenter Server sur la nouvelle machine, sélectionnez **View Composer est co-installé avec vCenter Server**.

      Si vous installez View Composer sur une machine autonome, sélectionnez **Serveur View Composer Server autonome** et fournissez le FQDN de la machine View Composer, ainsi que le nom d'utilisateur et le mot de passe de l'utilisateur de View Composer.

   e Dans le volet Domaines, cliquez sur **Vérifier les informations sur le serveur** et ajoutez ou modifiez les domaines View Composer si nécessaire.

   f 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 machines. 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 lisez les informations sur l'outil d'inscription ASP.NET IIS. Accédez à http://www.microsoft.com/net.

Procédure

1 Installez .NET Framework sur la machine physique ou virtuelle sur laquelle le service VMware Horizon View Composer associé à la base de données existante est installé.

2 Installez .NET Framework sur la machine de destination sur laquelle vous souhaitez installer le nouveau service VMware Horizon View Composer.

Suivant

Migrez le conteneur de clés RSA vers la machine de destination. Reportez-vous à la section « Migrer le conteneur de clés RSA vers le nouveau service View Composer », page 160.

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 la machine physique ou virtuelle source sur laquelle le service VMware Horizon View Composer existant réside vers la machine sur laquelle vous souhaitez installer le nouveau service VMware Horizon View Composer.

Vous devez effectuer cette procédure avant d'installer le nouveau service VMware Horizon View Composer.

Prérequis

Vérifiez que les outils d'enregistrement Microsoft .NET Framework et ASP.NET IIS sont installés sur les machines source et de destination. Reportez-vous à la section « Préparer Microsoft .NET Framework pour la migration de clés RSA », page 159.

Procédure

1 Sur la machine source sur laquelle réside le service VMware Horizon View Composer existant, ouvrez une invite de commande et accédez au répertoire `%windir%\Microsoft.NET\Framework\v2.0xxxxx`.

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 la machine de destination sur laquelle vous souhaitez installer le nouveau service VMware Horizon View Composer.

4 Sur la machine de destination, ouvrez une invite de commande et accédez au répertoire `%windir%\Microsoft.NET\Framework\v2.0xxxxx`.

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 cette machine et importées vers une autre machine. Si vous avez précédemment migré les clés vers cette machine 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 ultérieurement.

L'outil d'inscription importe les données de paire de clés dans le conteneur de clés local.

Suivant

Installez le nouveau service VMware Horizon View Composer sur la machine 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 VMware Horizon View Composer d'origine. Pour plus d'informations sur l'installation, consultez la section « Installation de View Composer » dans le document *Installation de View*.

Effectuez les étapes pour migrer View Composer vers une nouvelle machine et utiliser la même base de données. Reportez-vous à la section « Migrer View Composer avec une base de données existante », page 157.

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, reportez-vous à la section « Configurer le Serveur de connexion View, le serveur de sécurité ou View Composer afin d'utiliser un nouveau certificat SSL » dans le document *Installation de 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 enfichable Certificat a été ajouté à MMC sur l'ordinateur Windows Server sur lequel l'instance du Serveur de connexion View, le serveur de sécurité ou le service VMware Horizon View Composer a été installé.

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 VMware Horizon View Composer.
   b. Ouvrez une invite de commande Windows et accédez au fichier exécutable `SviConfig`.

      Le fichier est situé avec l'application View Composer. Le chemin d'accès par défaut est `C:\Program Files (x86)\VMware\VMware View Composer\sviconfig.exe`.

c Tapez la commande `SviConfig ReplaceCertificate`. Par exemple :

```
sviconfig –operation=ReplaceCertificate
          –delete=false
```

L'utilitaire affiche la liste numérotée des certificats SSL disponibles dans le magasin des certificats de l'ordinateur local Windows.

d Pour sélectionner un certificat, tapez le numéro du certificat et appuyez sur Entrée.

5 Si des certificats intermédiaires sont émis pour un hôte du 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 VMware Horizon View, Serveur de sécurité VMware Horizon View ou VMware Horizon View Composer pour que vos modifications prennent effet.

Informations collectées par le programme d'amélioration de l'expérience utilisateur

Vous pouvez participer à un programme d'amélioration du produit (Customer Experience improvement Program, CEIP). Si vous participez au programme, VMware collecte des données anonymes sur votre déploiement afin d'améliorer sa réponse aux besoins de ses clients. VMware utilise ces informations pour améliorer la qualité, la fiabilité et les performances de ses produits. Aucune donnée permettant d'identifier votre organisation n'est collectée.

La participation à ce programme est facultative. Vous pouvez choisir de ne pas participer en décochant l'option lorsque vous installez le Serveur de connexion View avec une nouvelle configuration. Si vous changez d'avis concernant le programme à tout moment après l'installation, il vous suffit de vous inscrire ou de vous retirer du programme en modifiant la page Attribution et utilisation de licence dans View Administrator.

Avant de collecter les données, VMware rend anonyme tous les champs contenant des informations spécifiques à votre organisation. Les champs expurgés identifient les ordinateurs, le stockage de données, les fonctionnalités de mise en réseau, les applications et les utilisateurs. Par exemple, les adresses IP et les spécifications de personnalisation de machine virtuelle 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 les changements apportés à la valeur lorsque vous modifiez votre environnement.

Pour vous aider à décider si vous souhaitez participer au programme, vous pouvez vérifier les champs auprès desquels VMware collecte les données. Vous pouvez également vérifier tous les champs expurgés. Les champs sont organisés par composant de View. Reportez-vous à « Données globales de View collectées par VMware », page 165 et aux rubriques connexes suivantes.

Protection de la confidentialité de VMware

VMware s'engage à protéger la confidentialité de vos informations personnelles et prend plusieurs mesures pour veiller à ce qu'aucune donnée recueillie par le programme d'amélioration du produit (customer experience improvement program, CEIP) n'inclue des informations sensibles susceptibles d'identifier de manière unique un client ou un utilisateur particulier. Ce programme ne recueille aucune information pouvant être utilisée pour vous identifier ou vous contacter. Aucune donnée identifiant votre entreprise ou vos utilisateurs n'est recueillie.

Lorsque la fonctionnalité CEIP est activée, le Serveur de connexion View rassemble des informations sur votre déploiement et exécute les actions suivantes sur les données :

1. Les données susceptibles d'identifier de manière unique votre déploiement, telles que des utilisateurs, des noms de serveurs, des adresses IP et des chemins de serveurs réseau, sont rendues anonymes en exécutant une fonction de hachage à sens unique sur les données. Cette méthode permet à VMware de rassembler des informations utiles sur la manière dont les serveurs, les machines et les utilisateurs uniques sont inclus dans votre déploiement sans recueillir de nom de serveur, de nom d'utilisateur et d'adresse spécifiques.
2. L'ensemble du jeu de données est chiffré à l'aide d'une clé publique. La clé privée requise pour déchiffrer le jeu de données est uniquement à la disposition de VMware.
3. Les informations rendues anonymes et chiffrées sont transmises à VMware à l'aide de HTTPS.

Vous pouvez vérifier la liste complète des champs auprès desquels les données sont collectées, ainsi que celle des champs rendus anonymes. Reportez-vous à « Données globales de View collectées par VMware », page 165 et aux rubriques connexes suivantes.

Prévisualiser les données collectées par le programme d'amélioration du produit

Vous pouvez prévisualiser les données que VMware est censé recevoir avant le chiffrement et la transmission de données. Lorsque vous activez cette option, le Serveur de connexion View écrit l'ensemble de données sur disque plutôt que de chiffrer et d'envoyer les données à VMware.

Vous configurez l'option permettant d'écrire les données CEIP sur un disque plutôt que de les transmettre à VMware en tant qu'option globale dans l'annuaire View LDAP. 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 du Serveur de connexion View, la modification est propagée à toutes les instances du Serveur de connexion View.

Procédure

1. Démarrez l'utilitaire ADSI Edit sur votre hôte du Serveur de connexion View.
2. Dans la boîte de dialogue Paramètres de connexion, sélectionnez **DC=vdi, DC=vmware, DC=int** ou connectez-vous à cet objet.
3. Dans le volet Ordinateur, sélectionnez ou tapez **`localhost:389`** ou le nom de domaine complet du Serveur de connexion View, suivi du port 389.

   Par exemple : `localhost:389 or mycomputer.mydomain.com:389`
4. Sur l'objet **CN=Common, OU=Global, OU=Properties**, définissez la valeur d'attribut **pae-ceipDumpOnly** sur 1.
5. Redémarrez le Serveur de connexion View.

Les fichiers de données CEIP sont écrits dans le format de texte brut JSON dans le répertoire `%PROGRAMFILES%\VMware\VMware View\Server\broker\temp\spool` sur l'instance du Serveur de connexion View.

Suivant

Pour rétablir le paramètre par défaut et commencer à envoyer les données à VMware, modifiez la valeur d'attribut **pae-ceipDumpOnly** à 0 et redémarrez le Serveur de connexion View.

Informations supplémentaires sur le programme d'amélioration du produit

Dès que vous acceptez de participer au programme d'amélioration du produit (Customer Experience Improvement Program, CEIP), des données sont collectées sur la première instance du Serveur de connexion View qui démarre au cours d'un déploiement de View. Les données de configuration sont collectées toutes les semaines. Les données de performances et d'utilisation sont collectées toutes les heures. Si l'instance du Serveur de connexion View n'a pas accès à Internet, les informations sont enregistrées sur le disque jusqu'à la prochaine connectivité Internet disponible.

Si vous acceptez de participer, vous pourrez changer d'avis plus tard. Vous pouvez vous inscrire ou mettre un terme à votre participation à tout moment en modifiant le paramètre **Envoyer des données anonymes à VMware** sur la page Licence produit et utilisation dans View Administrator. Pour que la modification prenne effet, redémarrez chaque instance du Serveur de connexion View de l'environnement.

La collecte de données par le programme d'amélioration du produit n'a aucune répercussion négative en termes de performances ou de consommation de disque sur votre déploiement de View. Les informations collectées et envoyées à VMware sont transmises à l'instance du Serveur de connexion View, que la fonctionnalité CEIP soit activée ou non. Par défaut, l'activation de la fonctionnalité peur consommer jusqu'à 100 Mo d'espace disque sur l'instance du Serveur de connexion View pour stocker les données avant de les envoyer à VMware. De même, les données non envoyées datant de plus de huit jours sont supprimées par défaut.

Si vos instances du Serveur de connexion View sont bloquées par un pare-feu qui les empêche d'accéder à Internet, vous pouvez toujours utiliser le CEIP. Lorsque le CEIP est activé, vos instances du Serveur de connexion View tentent régulièrement de se connecter avec le protocole HTTPS à l'URL de collecte des données à l'adresse `https://ceip.vmware.com`. Si la connexion est bloquée ou inaccessible en raison d'une limitation du serveur proxy ou du pare-feu, le Serveur de connexion View met en cache vos données CEIP jusqu'à ce que les enregistrements dépassent l'âge maximal configuré, huit jours par défaut, ou que les données collectées totales dépassent la taille maximale du spool, soit 100 Mo par défaut.

Vous pouvez modifier l'emplacement, la taille maximale et l'âge maximal du spool de données CEIP. L'emplacement et la taille du spool sont régis par les paramètres suivants dans la base de données View LDAP :

`pae-ceipSpoolDirectory`	Directory where CEIP data is cached before being sent to Vmware. Default: `Program Files\VMware\VMware View\Server\broker\temp\spool`
`pae-ceipMaxSpoolSize`	Maximum size, in bytes, of temporary spool data. Default: 100 MB
`pae-ceipMaxSpoolAge`	Maximum age of records in the temporary local spool. Default: 8 days

Vous ne serez pas contacté et vous ne recevrez pas de spam si vous participez au CEIP. Le CEIP ne collecte pas les renseignements personnels comme le nom, l'adresse personnelle, l'adresse e-mail ou le numéro de téléphone. Le CEIP ne vous demandera pas de participer à des enquêtes ou de lire du courrier indésirable, et vous ne serez pas contacté d'une autre manière.

Données globales de View collectées par VMware

Si vous vous inscrivez au programme d'amélioration du produit, VMware collecte des données globales concernant l'environnement View. Les champs contenant des informations sensibles restent anonymes.

Tableau 8-6. Informations sur les paramètres de configuration globale

Description	Ce champ reste-t-il anonyme ?	Exemple
Durée de vie maximale, en secondes, d'une session du Serveur de connexion View	Non	180 000
Durée, en secondes, avant que le Serveur de connexion View force la déconnexion des utilisateurs si aucune donnée n'est envoyée par le client	Non	36 000
Durée, en secondes, pendant laquelle un utilisateur peut être inactif avant que le Serveur de connexion View verrouille les informations d'identification de l'utilisateur pour l'authentification unique (Single Sign-On, SSO).	Non	900
Durée, en minutes, avant que les informations d'identification de SSO soient effacées pour les lancements de postes de travail	Non	-1 (ce qui signifie jamais)
Durée, en minutes, avant que les informations d'identification de SSO soient effacées pour les lancements d'applications	Non	-1 (ce qui signifie jamais)
Délai d'expiration de la session de la console View Administrator, en secondes	Non	3 000
Afficher un message de pré-ouverture de session lorsque les utilisateurs se connectent aux instances du Serveur de connexion View de cet espace	Non	0 ou 1
Le poste de travail distant peut exécuter un système d'exploitation serveur	Non	Vrai ou faux
Le serveur Mirage est activé	Non	Vrai ou faux
URL du serveur Mirage, incluant le numéro de port	Yes	Aucune
L'authentification unique réelle est-elle activée ?	Oui	Aucune
Un serveur d'inscription principal est-il configuré pour l'authentification unique réelle ?	Oui	Aucune
Un serveur d'inscription secondaire est-il configuré pour l'authentification unique réelle ?	Oui	Aucune

Tableau 8-7. Informations sur l'état global

Description	Ce champ reste-t-il anonyme ?	Exemple
Les serveurs View Server peuvent contacter le contrôleur du domaine.	Non	Vrai ou faux
DNS du domaine Active Directory	Yes	aucune
Le domaine est de style NT4.	Non	Vrai ou faux
Nom du domaine	Yes	Aucune
État du domaine	Non	OK
Type de relation d'approbation avec le domaine	Non	Domaine principal, bidirectionnelle, forêt bidirectionnelle, etc.

Données de Serveur de connexion View collectées par VMware

Si vous vous inscrivez au programme d'amélioration du produit, VMware collecte les données de certains champs du Serveur de connexion View. Les champs contenant des informations sensibles restent anonymes.

Tableau 8-8. Informations de configuration collectées auprès du Serveur de connexion View

Description	Ce champ reste-t-il anonyme ?	Exemple
Nom commun de l'entrée du Serveur de connexion View dans View LDAP	Yes	aucune
Le Serveur de connexion View est désactivé	Non	Vrai ou faux
L'authentification SecureID est configurée et active	Non	Vrai ou faux
L'authentification RADIUS est configurée et active	Non	Vrai ou faux
L'authentification de serveur SAML est autorisée, désactivée ou requise	Non	0 = Désactivée 1 = Autorisée 2 = Requise
Type d'installation du Serveur de connexion View	Non	0 = Serveur de connexion View 1 = Serveur de sécurité
Le nom de l'authentification SecureID doit-il correspondre au nom d'Active Directory ?	Non	True = Le nom de l'authentification SecureID est mappé False = Le nom de l'authentification SecureID n'est pas mappé
Les clients sont-ils autorisés à contourner le tunnel sécurisé ?	Non	Vrai ou faux
Les clients sont-ils autorisés à contourner PCoIP Secure Gateway ?	Non	Vrai ou faux
Configuration de l'authentification par carte à puce	Non	Désactivée, optionnelle ou requise
Les utilisateurs doivent-ils se déconnecter automatiquement lorsque leur carte à puce est retirée ?	Non	Vrai ou faux
Dossier dans lequel les sauvegardes de View LDAP sont stockées	Yes	aucune
Unité de temps de la configuration de la fréquence de sauvegarde de View LDAP	Non	Heure, jour ou semaine
Fréquence des sauvegardes de View LDAP	Non	Entier
Heure de la sauvegarde de View LDAP	Non	Entier
Nombre maximal de sauvegardes de View LDAP à stocker	Non	Entier
Heure de la dernière sauvegarde de View LDAP	Non	21 février 2014 12:00:10
État de la dernière sauvegarde de View LDAP	Non	OK
Sauvegarde urgente de View LDAP en attente	Non	Vrai ou faux
Balises associées à l'instance du Serveur de connexion View	Yes	aucune
Si l'instance du Serveur de connexion View est couplée à un serveur de sécurité	Non	0 = Non couplée 1 = Couplée
Nom unique de l'instance du Serveur de connexion View dans LDAP	Yes	aucune
Durée de validité du mot de passe de couplage du serveur de sécurité	Non	
Nom de l'hôte/du nœud de l'instance du Serveur de connexion View	Yes	aucune

Tableau 8-8. Informations de configuration collectées auprès du Serveur de connexion View (suite)

Description	Ce champ reste-t-il anonyme ?	Exemple
Numéro de version de l'instance du Serveur de connexion View uniquement	Non	6.0.0
Numéros de build et de version complets de l'instance du Serveur de connexion View	Non	6.0.0-123455
Reconnexion automatique à la passerelle sécurisée	Non	Vrai ou faux
Protocole client de tunnel	Non	
Protocole sur lequel l'instance du Serveur de connexion View ou le serveur de sécurité écoute	Non	

Tableau 8-9. Informations d'état collectées auprès du Serveur de connexion View

Description	Ce champ reste-t-il anonyme ?	Exemple
Numéro de build de l'instance du Serveur de connexion View	Non	123456
Nom du groupe répliqué du Serveur de connexion View, en général le premier nom de nœud de l'instance du Serveur de connexion View	`Yes`	aucune
Nom DNS de l'instance du Serveur de connexion View	`Yes`	aucune
Adresse IP de l'instance du Serveur de connexion View	`Yes`	aucune
Nom d'hôte NetBIOS de l'instance du Serveur de connexion View	`Yes`	aucune
Nombre de sessions actuellement sur cette instance du Serveur de connexion View	Non	Entier
Nombre maximal de sessions sur cette instance du Serveur de connexion View	Non	Entier
Nombre de sessions View Composer actuellement sur cette instance du Serveur de connexion View	Non	Entier
Nombre maximal de sessions View Composer sur cette instance du Serveur de connexion View	Non	Entier
Version de l'instance du Serveur de connexion View	Non	6.0.0

Tableau 8-10. Données d'utilisation dynamique collectées auprès du Serveur de connexion View

Description	Ce champ reste-t-il anonyme ?	Exemple
Nombre d'appels d'applets de commande PowerShell individuels	Non	Liste d'entiers
Nombre d'appels de méthodes d'API View individuelles dans la minute précédente	Non	Liste d'entiers
Taux de connexion, à l'aide de mots de passe, dans le temps	Non	Flottant
Taux de connexion, à l'aide du certificat de serveur SSL, dans le temps	Non	Flottant
Taux de connexion, à l'aide d'une authentification déléguée telle que SAML, dans le temps	Non	Flottant
Pourcentage moyen d'utilisation du CPU	Non	Entier
Pourcentage moyen d'utilisation de la mémoire	Non	Entier

Tableau 8-10. Données d'utilisation dynamique collectées auprès du Serveur de connexion View (suite)

Description	Ce champ reste-t-il anonyme ?	Exemple
Moyenne des connexions avec et sans mots de passe disponibles pour l'authentification unique	Non	Flottant
Nombre de démarrages de connexions de postes de travail avec chaque type de protocole d'affichage (PCoIP, RDP et VMware Blast)	Non	Liste d'entiers
Nombre de connexions d'un nouveau client à une application distante, pour chaque type de protocole d'affichage (PCoIP, RDP et VMware Blast)	Non	Liste d'entiers
Nombre de fois où le démarrage d'une application distante entraîne une nouvelle connexion, une connexion réutilisée, une connexion à une nouvelle session et une connexion à une session réutilisée	Non	Liste d'entiers
Nombre de démarrages de connexions de postes de travail pour un utilisateur autorisé à *n* nombres de postes de travail	Non	Liste des entiers, comme la liste du nombre d'utilisateurs autorisés à accéder à 1 poste de travail, 2 postes de travail, 3 postes de travail, etc.
Nombre de démarrages de connexions d'applications pour un utilisateur autorisé à *n* applications	Non	Liste d'entiers
Nombre de fois où *n* sessions de protocole (comme PCoIP) existent au moment où un utilisateur démarre une autre application. Par exemple, un utilisateur démarre une cinquième application, mais du fait que toutes les applications se trouvent dans la même batterie de serveurs, il n'existe qu'une seule session.	Non	Liste d'entiers, comme la liste du nombre d'utilisateurs ayant une session, du nombre d'utilisateurs ayant deux sessions, etc.

Données du serveur de sécurité collectées par VMware

Si vous participez au programme d'amélioration du produit, VMware collecte les données de certains champs du serveur de sécurité. Les champs contenant des informations sensibles restent anonymes.

Tableau 8-11. Informations du serveur de sécurité

Description	Ce champ reste-t-il anonyme ?	Exemple
Nombre de sessions PCoIP qui s'exécutent sur la passerelle sécurisée du serveur de sécurité	Non	Entier
Nombre de sessions de tout type qui s'exécutent sur la passerelle sécurisée du serveur de sécurité	Non	Entier
Numéro de build du serveur de sécurité	Non	123456
Nom d'hôte du serveur de sécurité	`Yes`	Aucune
IPsec est actif	Non	Vrai ou faux
La passerelle sécurisée est arrêtée	Non	Vrai ou faux
Nombre actuel de sessions	Non	Entier
URL de la passerelle sécurisée	`Yes`	Aucune
Numéro de version du serveur de sécurité	Non	6.0.0

Données de pool de postes de travail collectées par VMware

Si vous participez au programme d'amélioration du produit, VMware collecte les données de certains champs de pool de postes de travail. Les champs contenant des informations sensibles restent anonymes.

Tableau 8-12. Informations de configuration collectées à partir de pools de postes de travail

Description	Ce champ reste-t-il anonyme ?	Exemple
Nom commun de l'entrée du pool de postes de travail dans View LDAP	Yes	aucune
Nom d'affichage descriptif du pool de postes de travail	Yes	aucune
Le pool de postes de travail est désactivé	Non	Vrai ou faux
Type de pool de postes de travail	Non	L'un des types suivants : `IndividualVC`, `IndividualUnmanaged`, `Persistent`, `NonPersistent`, `SviPersistent`, `SviNonPersistent`, `ManualVCPersistent`, `Manual`, `ManualUnmanagedPersistent`, `ManualUnmanagedNonPersistent`, `TerminalService`, `OnRequestVcPersistent`, `OnRequestVcNonPersistent`, `OnRequestSviPersistent`, `OnRequestSviNonPersistent`
Dossier View Administrator sous lequel ce pool de postes de travail est groupé	Yes	aucune
Liste de noms uniques des machines virtuelles qui appartiennent au pool de postes de travail	Non	Exemple d'élément de la liste : `["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	Vrai ou faux
Les utilisateurs de ce pool de postes de travail sont-ils autorisés à réinitialiser leurs machines virtuelles ?	Non	Désactivée, optionnelle ou requise
Heure après laquelle un message de déconnexion forcée s'affiche	Non	Vrai ou faux
Nom unique de l'instance de vCenter Server qui gère les machines virtuelles du pool	Non	`"CN=e7a718de-d0f7-444a-9452-156dce289028,OU=VirtualCenter,OU=Properties,DC=vdi,DC=vmware,DC=int"`
Nombre minimal de machines virtuelles dans le pool de postes de travail	Non	Entier
Nombre maximal de machines virtuelles dans le pool de postes de travail	Non	Entier
Nombre de machines virtuelles de rechange provisionnées dans le pool de postes de travail	Non	Entier
Stratégie de suppression pour le pool de postes de travail	Non	Default, DeleteOnUse ou RefreshOnUse
Suffixe DNS utilisé dans le provisionnement	Yes	aucune

Tableau 8-12. Informations de configuration collectées à partir de pools de postes de travail (suite)

Description	Ce champ reste-t-il anonyme ?	Exemple
Mode d'attribution de nom (préfixe) à utiliser pour les noms de machines virtuelles déployées automatiquement	`Yes`	aucune
Modèle à partir duquel cloner des machines virtuelles	`Yes`	aucune
Dossier de vCenter Server dans lequel les machines virtuelles déployées sont stockées	`Yes`	aucune
Pool de ressources utilisé pour les machines virtuelles	`Yes`	aucune
Liste de banques de données	`Yes`	aucune
Spécification de personnalisation utilisée pour déployer des machines virtuelles	`Yes`	aucune
Activer le provisionnement automatique pour le pool de postes de travail	Non	Vrai ou faux
Erreurs rencontrées lors du provisionnement	Non	
Arrêter le provisionnement lorsqu'une erreur est rencontrée	Non	Vrai ou faux
Démarrer le provisionnement	Non	Vrai ou faux
Les valeurs du pool ont été calculées	Non	Vrai ou faux
Machine virtuelle parente utilisée pour provisionner des clones liés	`Yes`	Aucune
Nom du snapshot utilisé pour le provisionnement de clone lié	`Yes`	Aucune
ID du snapshot utilisé pour le provisionnement de clone lié	Non	`"snapshot-38685"`
ID du groupe de déploiement utilisé par le service VMware Horizon View Composer	Non	`"7119316f-00a8-463d-bbba-c3000f105aeb"`
Chemin d'accès à la banque de données du disque persistant de View Composer	`Yes`	aucune
Type de disque de View Composer	Non	`"SystemDisposable"`, `UserProfile`, etc.
Créer le disque persistant comme un disque fragmenté	Non	Vrai ou faux
Lettre de montage du lecteur pour le disque persistant ou le disque de données supprimables	Non	« `*` », « `C` », etc.
Taille cible du disque persistant	Non	Entier
Type de stratégie d'actualisation	Non	Toujours, Jamais ou Conditionnel
Seuil d'utilisation pour les opérations d'actualisation	Non	Entier
Seuil de temps pour les opérations d'actualisation	Non	Entier
Niveau de surcharge pour une banque de données qui stocke des clones liés	Non	Aucune, Classique, Modérée, Agressive
Chemin d'accès à une banque de données qui stocke des clones liés	`Yes`	aucune
Liste d'ID pour lesquels cette banque de données est utilisée	Non	Liste de GUID, tels que : `["7119316f-00a8-463d-bbba-c3000f105aeb"]`
État de machine virtuelle	Non	Prête, Pré-provisionnée, Clonage, Erreur de clonage, Personnalisation, Suppression, Maintenance, Erreur ou Déconnexion

Tableau 8-12. Informations de configuration collectées à partir de pools de postes de travail (suite)

Description	Ce champ reste-t-il anonyme ?	Exemple
Attribue une machine virtuelle à un utilisateur lorsque celui-ci se connecte pour la première fois	Non	Vrai ou faux
Indicateurs pour le pool de postes de travail	Non	
Paramètres de configuration multi-moniteur	Non	`svga.maxWidth:int`, `svga.vramSize:int`, `svga.maxHeight:int`, `svga.enable3d:bool`, `svga.numDisplays:int`
Une machine virtuelle individuelle a été convertie en un pool manuel	Non	Vrai ou faux
Le pool de clones liés utilise un clonage de snapshot natif avec VAAI	Non	Vrai ou faux
View Storage Accelerator (CBRC) est activé	Non	Vrai ou faux
Fréquence d'actualisation du cache CBRC	Non	Entier
Périodes d'interruption d'actualisation du cache CBRC	Non	Liste
Types de disque qui sont mis en cache pour CBRC (disques de système d'exploitation, disques persistants)	Non	Liste
La récupération d'espace disque de machine virtuelle (format fragmenté à optimisation d'espace) est activée	Non	Vrai ou faux
Seuil de récupération d'espace disque, en octets	Non	
Nombre minimal de machines virtuelles qui sont prêtes pendant une opération d'adaptation	Non	
Le pool de postes de travail utilise une banque de données Virtual SAN	Non	Vrai ou faux
Nombre de droits d'accès à des postes de travail distants pour ce pool de serveurs	Non	0 ou 1
Nombre de droits d'accès à des applications distantes pour ce pool	Non	0 ou 1
Protocole d'affichage par défaut	Non	PCoIP, RDP ou Blast
L'utilisateur peut choisir le protocole d'affichage utilisé	Non	Vrai ou faux
HTML Access est activé	Non	Vrai ou faux
Niveau de qualité de Flash	Non	Aucun utilisé, faible, moyen, élevé
Niveau de limitation de Flash	Non	Aucune utilisée, Classique, Modérée, Agressive
Le pool est désactivé	Non	Vrai ou faux
Le pool est marqué pour suppression	Non	Vrai ou faux
Balises associées à l'instance du Serveur de connexion View	`Yes`	aucune
Utiliser un serveur Mirage différent de celui spécifié dans les paramètres généraux	Non	Vrai ou faux
Le serveur Mirage est activé	Non	Vrai ou faux
URL du serveur Mirage, incluant le numéro de port	`Yes`	aucune
Nombre de clones par pool	Non	Entier

Données de machine collectées par VMware

Si vous vous inscrivez au programme d'amélioration du produit, VMware collecte les données des champs de View et de vCenter Server qui décrivent les machines virtuelles. Les champs contenant des informations sensibles restent anonymes.

Tableau 8-13. Données de machine collectées auprès de View

Description	Ce champ reste-t-il anonyme ?	Exemple
La machine a été marquée comme endommagée. La machine virtuelle a été utilisée alors que `useonce=true` et ne doit donc pas accepter de nouvelles sessions	Non	Vrai ou faux
Mappage de périphériques pour modifier des ID	Non	Un ensemble d'ID comme le suivant : `2000=01874583;01874583&2016=3910f513;3910f513`
Identifiant de la machine utilisée pour corréler les données	Non	vm-10
La personnalisation Sysprep est utilisée pour le système d'exploitation invité	Non	Vrai ou faux
Valeur du délai d'expiration. Laps de temps avant la déconnexion de la machine.	Non	Heure
ID aléatoire de View Agent ou Horizon Agent pour cette machine	Non	GUID
Diverses valeurs de configuration	Non	Entiers ou booléens (vrai ou faux)
Identifiant View LDAP du disque persistant précédent de View Composer	Non	Entrée LDAP
Applications ThinApp autorisées sur la machine	`Yes`	Aucune
Applications ThinApp qui attendent une désinstallation	`Yes`	Aucune
Applications ThinApp installées sur la machine	`Yes`	Aucune
État de la machine	Non	Non défini, Pré-provisionné, Clonage, Erreur de clonage, Personnalisation, Prêt, Suppression en cours, Maintenance, Erreur ou Déconnexion
Horodatage du démarrage de la personnalisation	Non	Entier
La machine est mise sous tension pour la personnalisation	Non	Entier. Les valeurs sont 0 ou 1.
La machine est sous tension	Non	Vrai ou faux
La machine est interrompue	Non	Vrai ou faux
L'état de la machine est en transition	Non	Vrai ou faux
La machine est configurée	Non	Vrai ou faux
Le chemin d'accès à la machine virtuelle dans vCenter Server	`Yes`	Aucune
Modèle de personnalisation utilisé pour personnaliser la machine	`Yes`	Aucune
ID de clone lié de View Composer pour la machine	Non	GUID du clone lié
La machine virtuelle est manquante dans vCenter Server	Non	Vrai ou faux
Nombre de tentatives de View pour mettre la machine hors tension	Non	Entier

Tableau 8-13. Données de machine collectées auprès de View (suite)

Description	Ce champ reste-t-il anonyme ?	Exemple
État du cache de lecture basé sur le contenu (View Storage Accelerator)	Non	Désactivé, Actuel, Obsolète ou Erreur
Heure de la dernière actualisation CBRC	Non	Date
Heure de la dernière erreur CBRC	Non	Entier
Heure de la dernière tentative incomplète de configuration de CBRC	Non	Entier
Version de View Agent ou d'Horizon Agent installée sur la machine	Non	6.0.0-551711
View Persona Management est activé sur la machine	Non	Vrai ou faux
Dernière quantité d'espace disque de la machine, en octets, récupérée (si le format de disque SE Sparse est utilisé)	Non	
Date et heure de la dernière récupération d'espace	Non	Horodatage

Tableau 8-14. Données de machine virtuelle collectées auprès de vCenter Server

Description	Ce champ reste-t-il anonyme ?	Exemple
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
Système d'exploitation installé sur la machine virtuelle	Non	Microsoft Windows 7 (32 bits), Microsoft Windows 8 (32 bits), Microsoft Windows Server 2008 R2 (64 bits), Microsoft Windows Server 2012 R2 (64 bits), etc.

Données de vCenter Server collectées par VMware

Si vous vous inscrivez au programme d'amélioration du produit, VMware collecte les données de certains champs de vCenter Server. Les champs contenant des informations sensibles restent anonymes.

Tableau 8-15. Informations sur le système hôte collectées auprès de vCenter Server

Description	Ce champ reste-t-il anonyme ?	Exemple
Heure à laquelle View a communiqué pour la dernière fois avec cet hôte vCenter Server	Non	Entier
URL de l'instance de vCenter Server	Yes	Aucune
Version de l'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

Tableau 8-16. Informations sur l'état de l'hôte collectées auprès de vCenter Server

Description	Ce champ reste-t-il anonyme ?	Exemple
Code d'état interne de l'état de la connexion entre vCenter Server et le Serveur de connexion View	Non	Status_Up
Description du code d'état de la connexion	Non	Connecté
Le certificat SSL de vCenter Server est valide	Non	Vrai ou faux
Raison pour laquelle le certificat SSL n'est pas valide	Non	Divergence de nom, non approuvé, impossible de vérifier la révocation, etc.

Tableau 8-17. Données de la banque de données collectées auprès de vCenter Server

Description	Ce champ reste-t-il anonyme ?	Exemple
Capacité de disque de cette banque de données	Non	Entier
Espace disque disponible sur cette banque de données	Non	Entier
Type de stockage	Non	NFS, VMFS
Plusieurs hôtes peuvent accéder à cette banque de données simultanément.	Non	Vrai ou faux

Tableau 8-18. Information sur le nœud ESX

Description	Ce champ reste-t-il anonyme ?	Exemple
Identifiant de vCenter Server qui gère un hôte ESXi particulier, accompagné de l'identifiant de l'hôte ESXi	Non	1234-ADEE-BECF-41AA-4950BCDA-host-14

Tableau 8-19. Informations sur le stockage en attachement direct d'un hôte ESXi

Description	Ce champ reste-t-il anonyme ?	Exemple
Fournisseur matériel du disque physique	Non	SEAGATE
Modèle du disque physique	Non	ST9300653SS
SSD	Non	Vrai ou faux
Capacité, en octets	Non	
Identifiant de l'hôte ESXi	Non	hôte-123
Identifiant de vCenter Server qui gère un hôte ESXi particulier	Non	1234-ADEE-BECF-41AA-4950BCDA

Données ThinApp collectées par VMware

Si vous participez au programme d'amélioration du produit, VMware collecte les données de certains champs ThinApp. Les champs contenant des informations sensibles restent anonymes.

Tableau 8-20. Informations sur ThinApp

Description	Ce champ reste-t-il anonyme ?	Type de valeur
Nom d'affichage du module ThinApp	Non	
Nombre de packages MSI associés à ThinApp	Non	Entier

Tableau 8-20. Informations sur ThinApp (suite)

Description	Ce champ reste-t-il anonyme ?	Type de valeur
Nombre d'attributions pour l'installation complète	Non	Entier
Liste des pools définis pour l'installation complète	Yes	Liste des hachages de noms communs
Postes de travail distants définis pour l'installation complète	Non	Liste des noms communs (GUID) de postes de travail
Nombre d'attributions pour la diffusion de l'application ThinApp	Non	Entier
Liste des pools définis pour diffuser l'application ThinApp	Yes	Liste des hachages de noms communs
Postes de travail distants définis pour la diffusion de l'application ThinApp	Non	Liste des noms communs (GUID) de postes de travail
ThinApp dans un groupe de pools définis pour l'installation complète	Non	Liste des ID d'applications ThinApp

Informations sur Architecture Cloud Pod collectées par VMware

Si vous vous inscrivez au programme d'amélioration du produit, VMware collecte les données de certains champs de Architecture Cloud Pod. Les champs contenant des informations sensibles restent anonymes.

Tableau 8-21. Informations collectées à propos de Architecture Cloud Pod

Description	Ce champ reste-t-il anonyme ?	Exemple ou type
La fonctionnalité Architecture Cloud Pod est activée	Non	Vrai ou faux
ID d'espace local	Non	
Fréquence, en secondes, à laquelle le système effectuera un contrôle de santé des espaces	Non	Entier
Différence de temps maximale autorisée entre les espaces, en secondes	Non	Entier
Nom commun du site auquel l'espace appartient	Non	
Liste des ID de droit d'accès global (par exemple, un espace dispose de pools de postes de travail prenant en charge les droits d'accès globaux)	Non	Liste de chaînes
Nom commun du point de terminaison de l'espace qui est une instance du Serveur de connexion View	Yes	
Nom commun de l'espace contenant ce point de terminaison	Non	
Le point de terminaison de l'espace est désactivé	Non	Vrai ou faux
Pondération à appliquer lors de la sélection aléatoire de points de terminaison (instances du Serveur de connexion View) pour les sessions distantes	Non	Entier
Le droit d'accès global est désactivé	Non	Vrai ou faux
La recherche de poste de travail démarre sur le site d'accueil de l'utilisateur (s'il est défini sur « faux », la recherche démarre sur l'espace local)	Non	Vrai ou faux
Le droit d'accès global concerne un poste de travail dédié	Non	0 = Non 1 = Oui
Étendue de la recherche à effectuer sur la session existante	Non	ANY, SITE ou LOCAL

Tableau 8-21. Informations collectées à propos de Architecture Cloud Pod (suite)

Description	Ce champ reste-t-il anonyme ?	Exemple ou type
Étendue du placement à effectuer sur la nouvelle session	Non	ANY, SITE ou LOCAL
Le site d'accueil de l'utilisateur est requis pour ce droit d'accès global	Non	Vrai ou faux
Le nettoyage automatique de session est activé	Non	Vrai ou faux

Données Horizon Client collectées par VMware

Si votre entreprise participe au programme d'amélioration du produit, VMware collecte des données provenant de certains champs d'Horizon Client. Les champs contenant des informations sensibles restent anonymes.

Bien que les informations soient chiffrées lors de leur transfert au Serveur de connexion, les informations sur le système client sont journalisées non chiffrées dans un répertoire propre à l'utilisateur. Les journaux ne contiennent aucune information d'identification personnelle.

Tableau 8-22. Données collectées depuis Horizon Client pour le programme d'amélioration du produit

Description	Ce champ reste-t-il anonyme ?	Exemple
Entreprise ayant produit l'application Horizon Client	Non	VMware
Nom du produit	Non	VMware Horizon Client
Version du produit client	Non	(Le format est *x.x.x-yyyyyy*, où *x.x.x* est le numéro de version du client et *yyyyyy* est le numéro de build.)
Architecture binaire du client	Non	Exemples : ■ i386 ■ x86_64 ■ arm
Nom du build du client	Non	Exemples : ■ VMware-Horizon-Client-Win32-Windows ■ VMware-Horizon-Client-Linux ■ VMware-Horizon-Client-iOS ■ VMware-Horizon-Client-Mac ■ VMware-Horizon-Client-Android ■ VMware-Horizon-Client-WinStore
Système d'exploitation hôte	Non	Exemples : ■ Windows 8.1 ■ Windows 7, 64 bits Service Pack 1 (Build 7601) ■ iPhone OS 5.1.1 (9B206) ■ Ubuntu 12.04.4 LTS ■ Mac OS X 10.8.5 (12F45)
Noyau du système d'exploitation hôte	Non	Exemples : ■ Windows 6.1.7601 SP1 ■ Darwin Kernel Version 11.0.0: Sun Apr 8 21:52:26 PDT 2012; root:xnu-1878.11.10~1/RELEASE_ARM_S5L8945X ■ Darwin 11.4.2 ■ Linux 2.6.32-44-generic #98-Ubuntu SMP Mon Sep 24 17:27:10 UTC 2012 ■ inconnu (pour Windows Store)

Tableau 8-22. Données collectées depuis Horizon Client pour le programme d'amélioration du produit (suite)

Description	Ce champ reste-t-il anonyme ?	Exemple
Architecture du système d'exploitation hôte	Non	Exemples : ■ x86_64 ■ i386 ■ armv71 ■ ARM
Modèle du système hôte	Non	Exemples : ■ Dell Inc. OptiPlex 960 ■ iPad3,3 ■ MacBookPro8,2 ■ Dell Inc. Precision WorkStation T3400 (A04 03/21/2008)
Processeur du système hôte	Non	Exemples : ■ Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GH ■ Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GH ■ inconnu (pour iPad)
Nombre de cœurs dans le processeur du système hôte	Non	Par exemple : 4
Mo de mémoire sur le système hôte	Non	Exemples : ■ 4096 ■ inconnu (pour Windows Store)
Nombre de périphériques USB connectés	Non	2 (la redirection de périphériques USB est prise en charge uniquement pour les clients Linux, Windows et Mac.)
Nombre maximal de connexions de périphériques USB simultanées	Non	2
ID de fournisseur de périphériques USB	Non	Exemples : ■ Kingston ■ NEC ■ Nokia ■ Wacom
ID de produit de périphérique USB	Non	Exemples : ■ DataTraveler ■ Gamepad ■ Disque de stockage ■ Souris sans fil
Famille de périphériques USB	Non	Exemples : ■ Sécurité ■ Périphérique d'interface humaine ■ Imagerie
Nombre d'utilisations du périphérique USB	Non	(Nombre de partages du périphérique)

Données collectées par VMware

Si votre entreprise participe au programme d'amélioration du produit, VMware collecte des données provenant de certains champs clients. Les champs contenant des informations sensibles restent anonymes.

Tableau 8-23. Données clientes collectées pour le programme d'amélioration du produit

Description	Nom de champ	Ce champ reste-t-il anonyme ?	Exemple
Entreprise qui a produit l'application	`<client-vendor>`	Non	VMware
Nom du produit	`<client-product>`	Non	
Version du produit client	`<client-version>`	Non	4.4.0-*build_number*
Architecture binaire du client	`<client-arch>`	Non	Exemples comprenant les valeurs suivantes : ■ navigateur ■ arm
Architecture native du navigateur	`<browser-arch>`	Non	Exemples comprenant les valeurs suivantes : ■ Win32 ■ Win64 ■ MacIntel ■ iPad
Chaîne de l'agent utilisateur du navigateur	`<browser-user-agent>`	Non	Exemples comprenant les valeurs suivantes : ■ Mozilla/5.0 (Windows NT 6.1; WOW64) ■ AppleWebKit/703.00 (KHTML, like Gecko) ■ Chrome/3.0.1750 ■ Safari/703.00 ■ Edge/13.10586
Chaîne de version interne de navigateur	`<browser-version>`	Non	Exemples comprenant les valeurs suivantes : ■ 7.0.3 (pour Safari), ■ 44.0 (pour Firefox) ■ 13.10586 (pour Edge)
Implémentation de base du navigateur	`<browser-core>`	Non	Exemples comprenant les valeurs suivantes : ■ Chrome ■ Safari ■ Firefox ■ Internet Explorer ■ Edge
Si le navigateur tourne sur un ordinateur de poche	`<browser-is-handheld>`	Non	true

Gestion de machines virtuelles de poste de travail de clone lié View Composer

9

Vous pouvez mettre à niveau des machines de poste de travail de clone lié View Composer, réduire la taille de leurs données de système d'exploitation et rééquilibrer les machines entre les magasins de données. Vous pouvez également gérer les disques persistants associés à des clones liés.

Ce chapitre aborde les rubriques suivantes :

Réduire la taille de clone lié avec une actualisation de machine

Une opération d'actualisation de machine restaure le disque du système d'exploitation de chaque clone lié à son état et à sa taille d'origine, ce qui réduit les coûts de stockage.

Si possible, planifiez les opérations d'actualisation au cours des heures creuses.

Pour obtenir des recommandations, reportez-vous à la section « Opérations d'actualisation de machine », page 180

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 s'il convient de forcer tous les utilisateurs à se déconnecter dès que l'opération commence ou d'attendre que chaque utilisateur se déconnecte avant d'actualiser le poste de travail de clone lié de cet utilisateur.

  Si vous forcez les utilisateurs à fermer leurs sessions, View informe les utilisateurs avant qu'ils soient déconnectés et les autorise à fermer leurs applications et leur session.

  Si vous forcez la déconnexion des utilisateurs, le nombre maximal d'opérations d'actualisation simultanées sur des postes de travail distants qui nécessitent une déconnexion correspond à la moitié de la valeur du paramètre **Nombre max. d'opérations de maintenance View Composer simultanées**. Par exemple, si ce paramètre est défini sur 24 et que vous forcez les utilisateurs à se déconnecter, le nombre maximal d'opérations d'actualisation simultanées sur les postes de travail distants qui nécessitent une déconnexion est de 12.

- Si votre déploiement comporte des instances répliquées du Serveur de connexion View, vérifiez que toutes les instances ont la même version.

Procédure

1 Dans View Administrator, sélectionnez **Catalogue > Pools de postes de travail**.

2 Sélectionnez le pool de postes de travail à actualiser en double-cliquant sur l'ID du pool dans la colonne de gauche.

3 Choisissez s'il convient d'actualiser plusieurs machines virtuelles ou une seule.

Option	Action
Pour actualiser toutes les machines virtuelles du pool de postes de travail	a Dans View Administrator, sélectionnez **Catalogue > Pools de postes de travail**. b Sélectionnez le pool de postes de travail à actualiser en double-cliquant sur l'ID du pool dans la colonne de gauche. c Sous l'onglet **Inventaire**, cliquez sur **Machines**. d Utilisez la touche Ctrl ou Maj pour sélectionner tous les ID de machine dans la colonne de gauche. e Sélectionnez **Actualiser** dans le menu déroulant de **View Composer**.
Pour actualiser une seule machine virtuelle	a Dans View Administrator, sélectionnez **Ressources > Machines**. b Sélectionnez la machine à actualiser en double-cliquant sur son ID dans la colonne de gauche. c Dans l'onglet **Résumé**, sélectionnez **Actualiser** dans le menu déroulant de **View Composer**.

4 Suivez les instructions de l'assistant.

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 contrôler l'opération en sélectionnant **Catalogue > Pools de postes de travail**, puis en double-cliquant sur l'ID de pool, et enfin en cliquant sur l'onglet **Tâches**. Vous pouvez cliquer sur **Annuler la tâche**, **Suspendre la tâche** ou **Reprendre la tâche** pour terminer une tâche, interrompre une tâche ou reprendre une tâche interrompue.

Opérations d'actualisation de machine

À mesure que les utilisateurs interagissent avec des clones liés, les disques de système d'exploitation des clones croissent. Une opération d'actualisation de machine restaure les disques de système d'exploitation à leur état et à leur taille d'origine, ce qui réduit 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.
- Une actualisation ne peut avoir lieu que lorsque les utilisateurs sont déconnectés de leurs postes de travail de clone lié.
- 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, Horizon 7 prend un nouveau snapshot du disque de 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 provisionnés et prêts lors d'opérations de View Composer » dans le document *Configuration des postes de travail virtuels dans Horizon 7*.

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 hors tension, Horizon 7 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 postes de travail de clone lié.

Mettre à jour des postes de travail de clone lié

Vous pouvez mettre à jour des machines virtuelles de clone lié en créant une image de base sur la machine virtuelle parente et en utilisant la fonctionnalité de recomposition pour distribuer l'image mise à jour aux clones liés.

- Préparer une machine virtuelle parente pour recomposer des clones liés page 182

  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 machines virtuelles de clone lié page 182

  La recomposition de machines met à jour simultanément toutes les machines virtuelles de clone lié ancrées à une machine virtuelle parente.
- Mise à jour de clones liés avec la recomposition page 184

  Dans une recomposition, vous pouvez fournir des correctifs de système d'exploitation, installer ou mettre à jour des applications, ou modifier les paramètres matériels de machines virtuelles dans tous les clones liés d'un pool de postes de travail.

- Corriger une recomposition échouée page 185

  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 clones liés

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 pour recomposer un clone lié de Windows 7.

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 machines virtuelles de clone lié

La recomposition de machines met à jour simultanément toutes les machines virtuelles de clone lié ancrées 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 clones liés », page 182.
- Familiarisez-vous avec les recommandations sur la recomposition. Reportez-vous à la section « Mise à jour de clones liés avec la recomposition », page 184.
- 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.
- Indiquez s'il convient de forcer tous les utilisateurs à fermer leur session dès le démarrage de la recomposition ou d'attendre que chaque utilisateur ferme sa session avant de recomposer son poste de travail de clone lié.

  Si vous forcez les utilisateurs à fermer leurs sessions, Horizon 7 informe les utilisateurs avant qu'ils soient déconnectés et les autorise à fermer leurs applications et leur session.

- Décidez d'arrêter l'apprivisionnement à la première erreur. Si vous sélectionnez cette option et qu'une erreur se produit lorsque View Composer provisionne un clone lié, le provisionnement s'arrête pour tous les clones du pool de postes de travail. 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 **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 le provisionnement du pool de postes de travail est activé. Lorsque le provisionnement du pool de postes de travail est désactivé, Horizon 7 empêche la personnalisation des postes de travail après leur recomposition.
- Si votre déploiement comporte des instances répliquées du Serveur de connexion Horizon, vérifiez que toutes les instances ont la même version.

Procédure

1 Indiquez s'il convient de recomposer l'intégralité du pool de postes de travail ou une seule machine.

Option	Action
Pour recomposer toutes les machines virtuelles du pool de postes de travail	a Dans Horizon Administrator, sélectionnez **Catalogue > Pools de postes de travail**. b Sélectionnez le pool de postes de travail à recomposer en double-cliquant sur l'ID du pool dans la colonne de gauche. c Sous l'onglet **Inventaire**, cliquez sur **Machines**. d Utilisez les touches Ctrl ou Maj pour sélectionner tous les ID de machines dans la colonne de gauche. e Sélectionnez **Recomposer** dans le menu déroulant **View Composer**.
Pour recomposer des machines virtuelles sélectionnées	a Dans Horizon Administrator, sélectionnez **Ressources > Machines**. b Sélectionnez la machine à recomposer en double-cliquant sur l'ID de la machine dans la colonne de gauche. c Dans l'onglet **Résumé**, sélectionnez **Recomposer** dans le menu déroulant **View Composer**.

2 Suivez les instructions de l'assistant.

  Vous pouvez sélectionner une nouvelle machine virtuelle à utiliser en tant que machine virtuelle parente du pool de postes de travail.

  Sur la page Ready to Complete, vous pouvez cliquer sur **Afficher les détails** pour afficher les postes de travail de clone lié qui seront recomposés.

Les machines virtuelles de clone lié sont actualisées et mises 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 machines virtuelles 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 Horizon Administrator, vous pouvez surveiller l'opération en cliquant sur **Catalogue > Pools de postes de travail**, en double-cliquant sur l'ID du pool et en cliquant sur l'onglet **Tâches**. Vous pouvez cliquer sur **Annuler la tâche**, **Suspendre la tâche** ou **Reprendre la tâche** pour terminer une tâche, interrompre une tâche ou reprendre une tâche interrompue.

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 » dans le document *Configuration des postes de travail virtuels dans Horizon 7*.

Mise à jour de clones liés avec la recomposition

Dans une recomposition, vous pouvez fournir des correctifs de système d'exploitation, installer ou mettre à jour des applications, ou modifier les paramètres matériels de machines virtuelles dans tous les clones liés d'un pool de postes de travail.

Pour recomposer des machines virtuelles de clone lié, vous mettez à jour la machine virtuelle parente dans vCenter Server ou sélectionnez une autre machine virtuelle qui deviendra 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 de postes de travail à attribution dédiée et à attribution 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 de postes de travail sont dérivés de différents snapshots de l'image de base ou d'images de base différentes, le pool de postes de travail comporte plusieurs réplicas.
- Une recomposition ne peut avoir lieu que lorsque les utilisateurs sont déconnectés de leurs postes de travail de clone lié.
- 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 provisionnés et prêts lors d'opérations de View Composer » dans le document *Configuration des postes de travail virtuels dans Horizon 7*.

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 » dans le document *Configuration des postes de travail virtuels dans Horizon 7*.

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

L'état des machines virtuelles est erroné ou périmé suite de l'échec d'une recomposition.

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 8 pour recomposer des clones liés de Windows 7.

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 de postes de travail.

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 machines virtuelles de clone lié.

Rééquilibrage des machines virtuelles de clone lié

Une opération de rééquilibrage redistribue de façon égale des machines virtuelles de clone lié sur des banques de données disponibles.

Vous pouvez également utiliser l'opération de rééquilibrage pour migrer des machines virtuelles de clone lié vers une autre banque de données. N'utilisez pas vSphere Client ou vCenter Server pour migrer ou gérer des machines virtuelles de clone lié. Reportez-vous à la section « Migrer des machines virtuelles de clone lié vers une autre banque de données », page 188.

Si possible, planifiez les opérations de rééquilibrage au cours des heures creuses.

Pour obtenir des recommandations, reportez-vous à la section « Rééquilibrage de clones liés sur des lecteurs logiques », page 187

Prérequis

- Familiarisez-vous avec l'opération de rééquilibrage. Reportez-vous à la section « Rééquilibrage de clones liés sur des lecteurs logiques », page 187.
- 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.
- Indiquez s'il convient 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 clone lié de cet utilisateur.

  Si vous forcez les utilisateurs à fermer leurs sessions, View 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 rééquilibrage simultanées sur les postes de travail distants nécessitant des fermetures de session est égal à la moitié de la valeur du paramètre **Nombre maximal d'opérations de maintenance View Composer simultanées**. Par exemple, si vous configurez ce paramètre sur 24 et que vous forcez les utilisateurs à fermer leur session, le nombre maximal d'opérations de rééquilibrage simultanées sur les postes de travail distants nécessitant une fermeture de session est de 12.
- Vérifiez que le provisionnement du pool de postes de travail est activé. Dans le cas contraire, View empêche la personnalisation des machines virtuelles après rééquilibrage.
- Si votre déploiement comporte des instances répliquées du Serveur de connexion View, vérifiez que toutes les instances ont la même version.

Procédure

1 Choisissez si vous devez rééquilibrer tout le pool ou une seule machine virtuelle.

Option	Action
Pour rééquilibrer toutes les machines virtuelles du pool	a Dans View Administrator, sélectionnez **Catalogue > Pools de postes de travail**. b Sélectionnez le pool à rééquilibrer en double-cliquant sur l'ID de pool dans la colonne de gauche. c Sous l'onglet **Inventaire**, cliquez sur **Machines**. d Utilisez les touches Ctrl ou Maj pour sélectionner plusieurs ou tous les ID de machines de la colonne de gauche. e Sélectionnez **Rééquilibrer** dans le menu déroulant **View Composer**.
Pour rééquilibrer une seule machine virtuelle	a Dans View Administrator, sélectionnez **Ressources > Machines**. b Sélectionnez la machine à rééquilibrer en double-cliquant sur l'ID de machine dans la colonne de gauche. c Dans l'onglet **Résumé**, sélectionnez **Rééquilibrer** dans le menu déroulant View Composer.

2 Suivez les instructions de l'assistant.

Les machines virtuelles de clone lié sont actualisées et rééquilibrées. Les disques du système d'exploitation sont réduits à leur taille d'origine.

Dans View Administrator, vous pouvez contrôler l'opération en sélectionnant **Catalogue > Pools de postes de travail**, en double-cliquant sur l'ID de pool et en cliquant sur l'onglet **Tâches**. Vous pouvez cliquer sur **Annuler la tâche**, **Suspendre la tâche** ou **Reprendre la tâche** pour terminer une tâche, interrompre une tâche ou reprendre une tâche interrompue.

Rééquilibrage de clones liés sur des lecteurs logiques

Une opération de rééquilibrage redistribue équitablement des machines virtuelles de clone lié entre les 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 la banque de données, Horizon 7 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 les recommandations suivantes aux rééquilibrages :

- Vous pouvez rééquilibrer des pools de postes de travail à attribution dédiée et à attribution 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 machines virtuelles 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 postes de travail de clone lié sur un hôte autonome et sélectionner une banque de données locale pour stocker les clones. Si vous modifiez le pool de postes de travail et sélectionnez un cluster et une banque de données partagée, toute opération de rééquilibrage échouera, car les hôtes du cluster ne peuvent pas accéder à la banque de données locale d'origine.
- Vous pouvez définir un nombre minimal de machines virtuelles provisionnées prêtes auxquelles les utilisateurs peuvent se connecter lors de l'opération de rééquilibrage. Reportez-vous à la section « Maintien des postes de travail de clone lié provisionnés et prêts lors d'opérations de View Composer » dans le document *Configuration des postes de travail virtuels dans Horizon 7*.

Important Si vous utilisez une banque de données Virtual SAN, vous ne pouvez utiliser l'opération de rééquilibrage que pour migrer toutes les machines virtuelles d'un pool de postes de travail vers un autre type de banques de données, ou l'inverse. Si un pool de postes de travail utilise une banque de données Virtual SAN, Virtual SAN fournit la fonctionnalité d'équilibrage de charge et optimise l'utilisation des ressources dans le cluster ESXi.

Migrer des machines virtuelles de clone lié vers une autre banque de données

Pour migrer des machines virtuelles de clone lié d'un ensemble de banques de données vers un autre, utilisez l'opération de rééquilibrage.

Lorsque vous utilisez un rééquilibrage, View Composer gère le déplacement des clones liés entre banques de données. View Composer s'assure que l'accès des clones liés au réplica est maintenu pendant et après l'opération de rééquilibrage. Si nécessaire, View Composer crée une instance du réplica sur la banque de données de destination.

Remarque N'utilisez pas vSphere Client ou vCenter Server pour migrer ou gérer des machines virtuelles de clone lié. N'utilisez pas Storage vMotion pour migrer des machines virtuelles de clone lié vers d'autres banques de données.

Prérequis

Familiarisez-vous avec l'opération de rééquilibrage. Reportez-vous aux sections « Rééquilibrage des machines virtuelles de clone lié », page 186 et « Rééquilibrage de clones liés sur des lecteurs logiques », page 187.

Procédure

1 Dans View Administrator, sélectionnez **Catalogue > Pools de postes de travail**, sélectionnez le pool de postes de travail à migrer, puis cliquez sur **Modifier**.

2 Dans l'onglet **Paramètres de vCenter**, effectuez un défilement vers le bas jusqu'à **Magasins de données**, puis cliquez sur **Parcourir**.

3 Dans la page Sélectionner des banques de données de clone lié, décochez les banques de données qui stockent actuellement les clones liés, cochez les banques de données de destination, puis cliquez sur **OK**.

4 Dans la fenêtre Modifier, cliquez sur **OK**.

5 Dans la page Pools de postes de travail, sélectionnez le pool en double-cliquant sur l'ID du pool dans la colonne de gauche.

6 Sélectionnez **Rééquilibrer** dans le menu déroulant **View Composer** et suivez les instructions de l'assistant pour rééquilibrer les machines virtuelles de clone lié.

Les machines virtuelles de clone lié sont actualisées et migrées vers les banques de données de destination.

Noms de fichier de disques de clone lié après une opération de rééquilibrage

Lorsque vous rééquilibrez des machines virtuelles de clone lié, vCenter Server modifie les noms de fichiers des disques persistants et des disques à données jetables View Composer des clones liés qui sont déplacés vers une nouvelle banque 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'une machine virtuelle de clone lié et l'attacher à un autre clone lié. Cette fonctionnalité vous permet de gérer des informations d'utilisateur séparément des machines virtuelles 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 distincts dans des machines virtuelles 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 » dans le document *Configuration des postes de travail virtuels dans Horizon 7*.

Vous pouvez détacher un disque persistant de sa machine virtuelle de clone lié et stocker le disque sur sa banque de données d'origine ou sur une autre banque de données. Après avoir détaché le disque, la machine virtuelle de clone lié est supprimée. Un disque persistant détaché n'est plus associé à aucune machine virtuelle.

Vous pouvez utiliser plusieurs méthodes pour attacher un disque persistant détaché à une autre machine virtuelle 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 possédant plusieurs postes de travail distants peut consolider les données utilisateur sur un seul poste de travail distant.
- 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 Les disques persistants doivent être reconnectés au système d'exploitation qui avait été utilisé lors de leur création. Par exemple, vous ne pouvez pas détacher un disque persistant d'un clone lié Windows 7 et recréer ou attacher le disque persistant à un clone lié Windows 8.

Horizon 7 peut gérer les disques persistants provenant de pools de clone lié créés dans View 4.5 ou version ultérieure. Les disques persistants créés dans les versions antérieures d'Horizon 7 ne peuvent pas être gérés et n'apparaissent pas sur la page Disques persistants d'Horizon Administrator.

Détacher un disque persistant de View Composer

Lorsque vous détachez un disque persistant de View Composer d'une machine virtuelle de clone lié, le disque est stocké et le clone lié est supprimé. Le fait de détacher un disque persistant vous permet de stocker et de réutiliser des informations spécifiques à l'utilisateur sur une autre machine virtuelle.

Procédure

1 Dans View Administrator, sélectionnez **Ressources > Disques persistants**.

2 Sélectionnez le disque persistant à détacher et cliquez sur **Détacher.**

3 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 une banque de données partagée ou une banque de données Virtual SAN. Si le disque persistant a été initialement stocké sur une banque de données Virtual SAN, vous pouvez sélectionner une banque de données Virtual SAN ou non-Virtual SAN pour stocker le disque persistant détaché. De même, si le disque persistant était stocké sur un réseau non-Virtual SAN, vous pouvez détacher le disque sur une banque de données non-Virtual SAN ou Virtual SAN.

Le disque persistant de View Composer est enregistré sur le magasin de données. La machine virtuelle de clone lié est supprimée et ne s'affiche pas dans View Administrator.

Attacher un disque persistant de View Composer à un autre clone lié

Vous pouvez attacher un disque persistant détaché à un autre machine virtuelle de clone lié. L'attachement d'un disque persistant rend les paramètres et les informations d'utilisateur du disque disponibles à l'utilisateur de l'autre machine virtuelle.

Vous attachez un disque persistant détaché comme disque secondaire sur la machine virtuelle de clone lié sélectionnée. Le nouvel utilisateur du clone lié a accès au disque secondaire et aux informations et paramètres d'utilisateur existants.

Vous ne pouvez pas attacher un disque persistant qui est stocké sur une banque de données non-Virtual SAN à une machine virtuelle qui est stockée sur une banque de données Virtual SAN. De même, vous ne pouvez pas attacher un disque qui est stocké sur une banque de données Virtual SAN à une machine virtuelle qui est stockée sur une banque de données non-Virtual SAN. View Administrator vous empêche de sélectionner des machines virtuelles stockées à la fois sur des banques de données Virtual SAN et non-Virtual SAN.

Pour déplacer un disque persistant détaché d'une banque de données non-Virtual SAN vers une banque de données Virtual SAN, vous pouvez récréer le disque sur une machine virtuelle qui est stockée sur une banque de données non-Virtual SAN et rééquilibrer le pool de postes de travail de la machine virtuelle vers une banque de données Virtual SAN. Reportez-vous à la section « Recréer un clone lié avec un disque persistant détaché », page 192.

Prérequis

- Vérifiez que la machine virtuelle sélectionnée utilise le même système d'exploitation que celui du clone lié dans lequel le disque persistant a été créé.

Procédure

1. Dans View Administrator, sélectionnez **Ressources > Disques persistants**.
2. Dans l'onglet **Détaché**, sélectionnez le disque persistant et cliquez sur **Attacher**.
3. Sélectionnez une machine virtuelle de clone lié à laquelle attacher le disque persistant.
4. Sélectionnez **Attacher comme disque secondaire**.
5. Cliquez sur **Terminer**.

Suivant

Assurez-vous que l'utilisateur du clone lié dispose de privilèges suffisants pour utiliser le disque secondaire attaché. Par exemple, si l'utilisateur d'origine dispose de certaines autorisations d'accès sur le disque persistant, et que le disque persistant est attaché en tant que lecteur `D` sur le nouveau clone lié, le nouvel utilisateur du clone lié doit disposer des autorisations d'accès de l'utilisateur d'origine sur le lecteur `D`.

Connectez-vous sur le système d'exploitation invité du clone lié en tant qu'administrateur et attribuez les privilèges appropriés au nouvel utilisateur.

Modifier le pool ou l'utilisateur d'un disque persistant de View Composer

Vous pouvez attribuer un disque persistant View Composer détaché à un nouveau pool de postes de travail ou à un nouvel utilisateur si le pool de postes de travail ou l'utilisateur d'origine a été supprimé de View.

Un disque persistant détaché est toujours associé à son pool de postes de travail ou à son utilisateur d'origine. Si le pool de postes de travail ou l'utilisateur est supprimé de View, vous ne pouvez pas utiliser le disque persistant pour recréer une machine virtuelle de clone lié.

En modifiant le pool de postes de travail et l'utilisateur, vous pouvez utiliser le disque persistant détaché pour recréer une machine virtuelle dans le nouveau pool de postes de travail. La machine virtuelle est attribuée au nouvel utilisateur.

Vous pouvez sélectionner un nouveau pool de postes de travail, un nouvel utilisateur, ou les deux.

Prérequis

- Vérifiez que le pool de postes de travail ou l'utilisateur du disque persistant a été supprimé de View.
- Vérifiez que le nouveau pool de postes de travail utilise le même système d'exploitation que le pool de postes de travail dans lequel le disque persistant a été créé.

Procédure

1 Dans View Administrator, sélectionnez **Ressources > Disques persistants**

2 Sélectionnez le disque persistant duquel l'utilisateur ou le pool de postes de travail a été supprimé et cliquez sur **Modifier**.

3 (Facultatif) Sélectionnez un pool de postes de travail de clone lié dans la liste.

4 (Facultatif) Sélectionnez un utilisateur pour le disque persistant.

Vous pouvez rechercher votre Active Directory pour le domaine et le nom d'utilisateur.

Suivant

Recréez une machine virtuelle de clone lié avec le disque persistant détaché.

Recréer un 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 la machine virtuelle de clone lié à partir du disque détaché.

Remarque Si vous recréez une machine virtuelle de clone lié dans un pool de postes de travail qui a atteint sa taille maximale, la machine virtuelle recréée est toujours ajoutée au pool de postes de travail. La taille du pool de postes de travail dépasse la taille maximale spécifiée.

Si un pool de postes de travail ou un utilisateur d'origine d'un disque persistant a été supprimé de View, vous pouvez en attribuer un nouveau au disque persistant. Reportez-vous à la section « Modifier le pool ou l'utilisateur d'un disque persistant de View Composer », page 191.

View ne prend pas en charge la recréation d'une machine virtuelle avec un disque persistant qui est stocké sur une banque de données non-Virtual SAN si la nouvelle machine virtuelle est stockée sur une banque de données Virtual SAN. De même, si le disque persistant est stocké sur une banque de données Virtual SAN, View ne prend pas en charge la recréation d'une machine virtuelle sur une banque de données non-Virtual SAN.

Pour déplacer un disque persistant détaché d'une banque de données non-Virtual SAN vers une banque de données Virtual SAN, vous pouvez récréer le disque sur une machine virtuelle qui est stockée sur une banque de données non-Virtual SAN et rééquilibrer le pool de postes de travail de la machine virtuelle vers une banque de données Virtual SAN.

Procédure

1 Dans View Administrator, sélectionnez **Ressources > Disques persistants**.

2 Dans l'onglet **Détaché**, sélectionnez le disque persistant et cliquez sur **Récréer la machine**.

Vous pouvez sélectionner plusieurs disques persistants pour recréer une machine virtuelle de clone lié pour chaque disque.

3 Cliquez sur **OK**.

View crée une machine virtuelle de clone lié pour chaque disque persistant que vous sélectionnez et ajoute la machine virtuelle au pool de postes de travail d'origine.

Les disques persistants restent sur le magasin de données sur lequel ils étaient stockés.

Restaurer un clone lié en important un disque persistant à partir de vSphere

Si une machine virtuelle de clone lié devient inaccessible dans View, vous pouvez la restaurer si elle a été configurée avec un disque persistant de View Composer. Vous pouvez importer le disque persistant à partir d'une banque de données vSphere dans View.

Vous importez le fichier de disque persistant dans View en tant que disque persistant détaché. Vous pouvez attacher le disque détaché à une machine virtuelle existante ou recréer le clone lié d'origine dans View.

Procédure

1 Dans View Administrator, sélectionnez **Ressources > Disques persistants**.

2 Dans l'onglet **Détaché**, cliquez sur **Importer depuis vCenter**.

3 Sélectionnez une instance de vCenter Server.

4 Sélectionnez le datacenter où se situe le fichier disque.

5 Sélectionnez un pool de postes de travail de clone lié dans lequel créer une nouvelle machine virtuelle de clone lié avec le disque persistant.

6 Dans la zone de texte **Fichier de disque persistant**, cliquez sur **Parcourir**, cliquez sur la flèche vers le bas, puis sélectionnez une banque 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.

7 Cliquez sur le nom de magasin de données pour afficher ses fichiers de stockage de disque et ses fichiers de machine virtuelle.

8 Sélectionnez le fichier disque persistant que vous voulez importer.

9 Dans la zone de texte **Utilisateur**, cliquez sur **Parcourir**, sélectionnez l'utilisateur auquel attribuer la machine virtuelle, puis cliquez sur **OK**.

Le fichier de disque est importé dans View en tant que disque persistant détaché.

Suivant

Pour restaurer la machine virtuelle de clone lié, vous pouvez recréer la machine virtuelle d'origine ou attacher le disque persistant détaché à une autre machine virtuelle.

Pour plus d'informations, reportez-vous à « Recréer un clone lié avec un disque persistant détaché », page 192 et à « Attacher un disque persistant de View Composer à un autre clone lié », page 191.

Supprimer un disque persistant détaché de View Composer

Lorsque vous supprimez un disque persistant détaché, vous pouvez supprimer le disque de View et le laisser sur la banque de données ou supprimer le disque de View et de la banque de données.

Procédure

1 Dans View Administrator, sélectionnez **Ressources > Disques persistants**.

2 Dans l'onglet **Détaché**, sélectionnez le disque persistant et cliquez sur **Supprimer**.

3 Indiquez si vous souhaitez supprimer le disque de la banque de données ou le laisser dans la banque de données après l'avoir supprimé de View.

Option	Description
Supprimer du disque	Après la suppression, le disque persistant n'existe plus.
Supprimer de View uniquement	Après sa suppression, le disque persistant n'est plus accessible dans View mais demeure dans la banque de données.

4 Cliquez sur **OK**.

Gestion de pools de postes de travail, de machines et de sessions 10

Dans View Administrator, vous pouvez gérer des pools de postes de travail, des postes de travail basés sur une machine virtuelle, des postes de travail basés sur une machine physique, des sessions de poste de travail et des sessions d'application.

Ce chapitre aborde les rubriques suivantes :

Gestion des pools de postes de travail Instant Clone

Dans View Administrator, vous pouvez effectuer des tâches administratives sur un pool de postes de travail Instant Clone, telles que la planification d'une opération d'image de transfert.

Modifier l'image d'un pool de postes de travail de clone instantané

Vous pouvez modifier l'image d'un pool de postes de travail Instant Clone pour transférer les modifications ou pour restaurer une image précédente. Vous pouvez sélectionner n'importe quel snapshot depuis n'importe quelle machine virtuelle comme nouvelle image.

Procédure

1 Dans Horizon Administrator, sélectionnez **Catalogue > Pools de postes de travail**

2 Double-cliquez sur l'ID de pool.

3 Sélectionnez **Image de transfert > Planifier**.

La fenêtre Planifier l'image de transfert s'ouvre.

4 Suivez les invites.

Vous pouvez planifier la tâche pour qu'elle démarre immédiatement ou ultérieurement. Pour les clones avec des sessions d'utilisateur, vous pouvez spécifier si vous voulez forcer les utilisateurs à fermer leur session ou à attendre. Lorsque les utilisateurs ferment leur session, Horizon 7 recrée les clones.

5 Sur la page Prêt à terminer, cliquez sur **Afficher les détails** pour voir la liste de postes de travail dans le pool.

Après avoir initié cette opération, la publication de la nouvelle image démarre immédiatement. Pour plus d'informations sur la publication, reportez-vous à la section « Pools de postes de travail de clone instantané » dans le document *Configuration des postes de travail virtuels dans Horizon 7*. La recréation de clones démarre au moment que vous avez spécifié dans l'assistant Planifier l'image de transfert.

Surveiller une opération d'image de transfert

Vous pouvez surveiller la progression d'une opération d'image de transfert sur un pool de postes de travail Instant Clone dans View Administrator.

Procédure

1 Dans View Administrator, sélectionnez **Catalogue > Pools de postes de travail**.

2 Double-cliquez sur l'ID du pool.

L'onglet **Résumé** affiche les informations sur l'image actuelle et sur l'image en attente.

3 Cliquez sur l'onglet **Tâches**.

La liste des tâches associées à l'opération d'image de transfert apparaît.

Replanifier ou annuler une opération d'image de transfert

Vous pouvez replanifier ou annuler une opération d'image de transfert sur un pool de postes de travail Instant Clone dans View Administrator.

Procédure

1 Dans View Administrator, sélectionnez **Catalogue > Pools de postes de travail**.

2 Double-cliquez sur l'ID du pool.

L'onglet **Résumé** affiche les informations sur l'image actuelle et sur l'image en attente.

3 Sélectionnez **Image de transfert > Replanifier** ou **Image de transfert > Annuler**.

4 Suivez les invites.

Si vous annulez l'opération d'image de transfert alors que la création de clones est en cours, les clones avec la nouvelle image restent dans le pool et le pool contient un mélange de clones, certains avec la nouvelle image et les autres avec l'ancienne. Pour vous assurer que tous les clones ont bien la même image, vous pouvez supprimer tous les clones. View recrée les clones avec la même image.

Gestion de pools de postes de travail

Dans View Administrator, vous pouvez effectuer des tâches administratives sur un pool de postes de travail, telles que modifier ses propriétés, activer, désactiver ou supprimer le pool.

Modifier un pool de postes de travail

Vous pouvez modifier un pool de postes de travail existant pour configurer des paramètres comme le nombre de machines de rechange, les banques de données et les spécifications de personnalisation.

Prérequis

Familiarisez-vous avec les paramètres de pool de postes de travail que vous pouvez ou non modifier après la création d'un pool. Reportez-vous aux sections « Modification des paramètres dans un pool de postes de travail existant », page 197 et « Paramètres fixes dans un pool de postes de travail existant », page 199.

Procédure

1 Dans View Administrator, sélectionnez **Catalogue > Pools de postes de travail**.

2 Sélectionnez un pool de postes de travail et cliquez sur **Modifier**.

3 Cliquez sur un onglet dans la boîte de dialogue Modifier et reconfigurez des options de pool de postes de travail.

4 Cliquez sur **OK**.

Si vous modifiez l'image d'un pool de postes de travail de clone instantané, l'opération de publication d'image démarre immédiatement. Dans View Administrator, la page de résumé du pool de postes de travail indique que l'état de l'image en attente est `Publication – Modification de l'infrastructure`.

Si vous modifiez le cluster d'un pool de postes de travail de clone instantané, de nouvelles machines virtuelles réplica et parente sont créées dans le nouveau cluster. Vous pouvez initier une image de transfert à l'aide de la même image pour que de nouveaux clones soient créés dans le nouveau cluster. Toutefois, la machine virtuelle modèle, qui est utilisée pour le processus de clonage, reste dans l'ancien cluster. Vous pouvez passer l'hôte ESXi sur lequel se trouve la machine virtuelle modèle en mode de maintenance, mais vous ne pouvez pas migrer la machine virtuelle modèle. Pour supprimer complètement toutes les machines virtuelles d'infrastructure, notamment la machine virtuelle modèle, de l'ancien cluster, vous pouvez initier une image de transfert à l'aide d'une nouvelle image.

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 10-1. Paramètres modifiables dans un pool de postes de travail existant

Onglet Configuration	Description
Général	Modifiez les options de dénomination de pool de postes de travail et les paramètres de gestion des stratégies de stockage. Les paramètres de gestion des stratégies de stockage déterminent s'il convient d'utiliser une banque de données Virtual SAN. Si vous n'utilisez pas Virtual SAN, vous pouvez sélectionner des banques de données distinctes pour les disques de réplica et de système d'exploitation. **Remarque** Pour les clones liés View Composer, si vous optez pour l'utilisation de Virtual SAN, vous devez effectuer une opération de rééquilibrage pour migrer toutes les machines virtuelles du pool de postes de travail vers la banque de données Virtual SAN.
Paramètres du pool de postes de travail	Modifiez les paramètres de machine, tels que la stratégie d'alimentation, le protocole d'affichage et les paramètres Adobe Flash. Dans Horizon 7.0, la stratégie d'alimentation n'est pas prise en charge pour les clones instantanés.
Paramètres de provisionnement	Modifiez les options de provisionnement de pool de postes de travail et ajoutez des machines au pool de postes de travail. Cet onglet n'est disponible que pour les pools de postes de travail 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 de postes de travail automatisés.

Tableau 10-1. Paramètres modifiables dans un pool de postes de travail existant (suite)

Onglet Configuration	Description
Personnalisation d'invité	Si Sysprep était sélectionné, vous pouvez modifier la spécification de personnalisation. Dans Horizon 7.0, Sysprep n'est pas disponible pour les clones instantanés. Si QuickPrep était sélectionné, vous pouvez modifier le domaine et le conteneur Active Directory et spécifier les scripts de mise hors tension et de post-synchronisation. Si ClonePrep était sélectionné, vous pouvez modifier le conteneur Active Directory et spécifier les scripts de mise hors tension et de post-synchronisation. Vous ne pouvez pas modifier le domaine. **Remarque** Pour les clones instantanés, si vous modifiez le nom du script de mise hors tension ou de post-synchronisation, ou leurs paramètres, et que le nouveau script existe dans l'image actuelle, le nouveau script est exécuté et les nouveaux paramètres sont utilisés lorsqu'un clone est créé. Si le nouveau script n'existe pas dans l'image actuelle, vous devez sélectionner ou créer une image disposant du nouveau script et exécuter une image de transfert. Pour les clones liés View Composer, si vous modifiez le nom du script de mise hors tension ou de post-synchronisation, la modification s'applique lors de la prochaine opération de recomposition. Toutefois, les modifications apportées aux paramètres du script de mise hors tension ou de post-synchronisation ne s'appliquent pas aux clones créés avec le snapshot actuel. Cet onglet n'est disponible que pour les pools de postes de travail automatisés.
Stockage avancé > Utiliser View Storage Accelerator	Si vous cochez ou décochez la case **Utiliser View Storage Accelerator**, si vous effectuez une replanification lorsque les fichiers condensés de View Storage Accelerator sont régénérés, les paramètres affectent les machines virtuelles existantes. Si vous modifiez les paramètres de View Storage Accelerator pour un pool de postes de travail existant, les modifications ne prendront pas effet avant d'avoir éteint les machines virtuelles du pool de postes de travail. Reportez-vous à la section « Configurer View Storage Accelerator pour des clones liés de View Composer » dans le document *Configuration des postes de travail virtuels dans Horizon 7*. **Remarque** Si vous sélectionnez **Utiliser View Storage Accelerator** sur un pool de postes de travail de clone lié existant et si le réplica n'était pas précédemment activé pour View Storage Accelerator, cette fonctionnalité 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 de postes de travail sur une nouvelle machine virtuelle parente. Cette option est automatiquement activée sur les clones instantanés.
Stockage avancé > Récupérer l'espace disque de machine virtuelle	Si vous cochez ou décochez **Récupérer de l'espace disque de VM**, ou replanifiez à quel moment la récupération d'espace disque de machine virtuelle se produit, les nouveaux paramètres affectent les machines virtuelles existantes si elles ont été créées avec des disques à optimisation d'espace. Reportez-vous à la section « Récupérer de l'espace disque sur des machines virtuelles de clone lié » dans le document *Configuration des postes de travail virtuels dans Horizon 7*. Cette option ne s'applique pas aux clones instantanés.

Tableau 10-1. Paramètres modifiables dans un pool de postes de travail existant (suite)

Onglet Configuration	Description
Stockage avancé > Utiliser des snapshots NFS natifs (VAAI)	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) » dans le document *Configuration des postes de travail virtuels dans Horizon 7*. Cette option n'est pas prise en charge pour les clones instantanés.
Stockage avancé > Portée du partage de page transparente	Si vous modifiez le paramètre **Portée de partage de page transparente**, le nouveau paramètre s'applique lors de la prochaine mise sous tension de la machine virtuelle. Sélectionnez le niveau auquel autoriser le partage de page transparente (TPS). Les choix sont **Machine virtuelle** (par défaut), **Pool**, **Espace** ou **Global**. Si vous activez le partage de page transparente pour les machines du pool, de l'espace ou globalement, l'hôte ESXi élimine les copies redondantes des pages mémoire obtenues si les machines utilisent le même système d'exploitation invité ou les mêmes applications. Le partage de page se produit sur l'hôte ESXi. Par exemple, si vous activez le partage de page transparente au niveau du pool alors que le pool couvre plusieurs hôtes ESXi, seules les machines virtuelles sur le même hôte et à l'intérieur du même pool partageront des pages. Au niveau global, toutes les machines gérées par Horizon 7 sur le même hôte ESXi peuvent partager des pages de mémoire, quel que soit le pool sur lequel résident les machines. **Remarque** Par défaut, les pages de mémoire ne sont pas partagées entre plusieurs machines, car le partage de page transparente (TPS) peut créer un risque. Les recherches indiquent que le partage de page transparente peut être exploité de façon abusive pour obtenir un accès non autorisé à des données dans des scénarios de configuration très limités. Cette option est automatiquement activée sur les clones instantanés.

Si vous modifiez un pool de postes de travail de clone instantané pour ajouter ou supprimer des banques de données, le rééquilibrage des machines virtuelles se produit automatiquement lorsqu'un nouveau clone doit être créé, par exemple, lorsqu'un utilisateur se déconnecte ou que vous augmentez la taille du pool. Si vous voulez que le rééquilibrage arrive plus vite, procédez comme suit :

- Si vous supprimez une banque de données, supprimez manuellement les postes de travail sur cette banque de données pour que les nouveaux postes de travail soient créés sur les banques de données restantes.
- Si vous ajoutez une banque de données, supprimez manuellement quelques postes de travail des banques de données d'origine pour que les nouveaux postes de travail soient créés sur la nouvelle banque de données. Vous pouvez également supprimer tous les postes de travail pour que, lorsqu'ils sont recréés, ils soient distribués uniformément sur les banques de données.

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 10-2. Paramètres fixes dans un pool de postes de travail existant

Paramètre	Description
Pool type (Type de pool)	Une fois un pool de postes de travail automatisé, manuel ou RDS créé, vous ne pouvez pas modifier le type du pool.
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 alterner entre machines virtuelles complètes et machines virtuelles de clone lié.
ID du pool	Vous ne pouvez pas modifier l'ID de pool.

Tableau 10-2. Paramètres fixes dans un pool de postes de travail existant (suite)

Paramètre	Description
Méthode de dénomination et de provisionnement de machine	Pour ajouter des machines virtuelles à un pool de postes de travail, vous devez faire appel à la méthode de provisionnement qui a été utilisée pour créer le pool. Vous ne pouvez pas alterner entre la spécification manuelle des noms de machine et l'utilisation d'un mode d'attribution de nom. Si vous spécifiez des noms manuellement, vous pouvez ajouter des noms à la liste des noms de machines. Si vous utilisez un mode d'attribution de nom, vous pouvez augmenter le nombre maximal de machines.
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 Modifier, mais les valeurs n'affectent que les nouvelles machines virtuelles créées après la modification des paramètres.
disques persistants de View Composer	Vous ne pouvez pas configurer des disques persistants après la création d'un pool de postes de travail de clone lié sans disques persistants.
View Composer customization method (Méthode de personnalisation de View Composer)	Après avoir personnalisé un pool de postes de travail de clone lié avec QuickPrep ou Sysprep, vous ne pouvez pas passer à l'autre méthode de personnalisation pour créer ou recomposer les machines virtuelles du pool.

Modifier la taille d'un pool automatisé approvisionné par un mode d'attribution de nom

Lorsque vous provisionnez un pool de postes de travail automatisé à l'aide d'un mode d'attribution de nom, vous pouvez augmenter ou diminuer la taille du pool en modifiant le nombre maximal de machines.

Prérequis

- Vérifiez que vous avez provisionné le pool de postes de travail à l'aide d'un mode d'attribution de nom. Si vous spécifiez manuellement des noms de machines, consultez « Ajouter des machines à un pool automatisé provisionné par une liste de noms », page 201
- Vérifiez que le pool de postes de travail est automatisé.

Procédure

1 Dans View Administrator, sélectionnez **Catalogue > Pools de postes de travail**.

2 Sélectionnez le pool de postes de travail et cliquez sur **Modifier**.

3 Dans l'onglet **Paramètres d'approvisionnement**, tapez le nouveau nombre de machines du pool de postes de travail dans la zone de texte **Nombre max. de machines**.

Si vous augmentez la taille du pool de postes de travail, vous pouvez y ajouter des nouvelles machines jusqu'à la limite maximale autorisée.

Si vous diminuez la taille d'un pool à attribution flottante, les machines inutilisées sont supprimées. 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 à attribution dédiée, les machines non attribuées sont supprimées. Si le nombre d'utilisateurs attribués à des machines est supérieur au nouveau nombre maximal, la taille du pool diminue dès que vous supprimez l'attribution d'utilisateurs.

Remarque Lorsque vous diminuez la taille d'un pool de postes de travail, le nombre réel de machines peut être supérieur à la valeur **Nombre max. de machines** si le nombre d'utilisateurs dont la session est ouverte ou qui sont attribués à des machines est supérieur à la valeur spécifiée dans **Nombre max. de machines**.

Ajouter des machines à un pool automatisé provisionné par une liste de noms

Pour ajouter des machines à un pool de postes de travail automatisé provisionné en spécifiant manuellement les noms des machines, vous fournissez une autre liste de nouveaux noms de machines. Cette fonction vous permet de développer un pool de postes de travail et de continuer à utiliser les conventions de dénomination de votre entreprise.

Dans Horizon 7.0, cette fonctionnalité n'est pas prise en charge pour les clones instantanés.

Suivez les instructions suivantes pour ajouter manuellement les noms des machines :

- Tapez chaque nom de machine sur une ligne distincte.
- Un nom de machine peut comporter jusqu'à 15 caractères alphanumériques.
- Vous pouvez ajouter un nom d'utilisateur à chaque entrée de machine. Utilisez une virgule pour séparer le nom d'utilisateur de celui de la machine.

Dans cet exemple, deux machines sont ajoutées. La deuxième machine est associée à un utilisateur :

```
Desktop-001
Desktop-002,abccorp.com/jdoe
```

Remarque Dans un pool à attribution flottante, vous ne pouvez pas associer des noms d'utilisateurs à des noms de machines. Les machines ne sont pas dédiées aux utilisateurs associés. Dans un pool à attribution flottante, toutes les machines qui ne sont pas utilisées actuellement restent accessibles à tout utilisateur ouvrant une session.

Prérequis

Vérifiez que vous avez créé le pool de postes de travail en spécifiant manuellement les noms des machines. Vous ne pouvez pas ajouter des machines en fournissant de nouveaux noms de machines si vous avez créé le pool en désignant un mode d'attribution de nom.

Procédure

1 Créez un fichier texte contenant la liste des noms de machines supplémentaires.

Si vous prévoyez d'ajouter seulement quelques machines, vous pouvez taper les noms de machines directement dans l'assistant Ajouter un pool de postes de travail. Vous n'avez pas à créer un fichier texte séparé.

2 Dans View Administrator, sélectionnez **Catalogue > Pools de postes de travail**.

3 Sélectionnez le pool de postes de travail à étendre.

4 Cliquez sur **Modifier**.

5 Cliquez sur l'onglet **Paramètres d'approvisionnement**.

6 Cliquez sur **Ajouter des machines**.

7 Copiez votre liste de noms de machines dans la page Entrer des noms de machine et cliquez sur **Suivant**.

L'assistant Entrer des noms de machine affiche la liste des machines et indique les erreurs de validation avec un **X** rouge.

8 Corrigez les noms de machines 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 **Précédent**.

c Modifiez les noms incorrects et cliquez sur **Suivant**.

9 Cliquez sur **Terminer**.

10 Cliquez sur **OK**.

Dans vCenter Server, vous pouvez surveiller la création des nouvelles machines virtuelles.

Dans View Administrator, vous pouvez afficher les machines à mesure de leur ajout au pool de postes de travail en sélectionnant **Catalogue > Pools de postes de travail**.

Désactiver ou activer un pool de postes de travail

Lorsque vous désactivez un pool de postes de travail, celui-ci n'est plus présenté aux utilisateurs et le provisionnement de pool s'arrête. Les utilisateurs n'ont plus accès au pool. Après avoir désactivé un pool, vous pouvez l'activer de nouveau.

Vous pouvez désactiver un pool de postes de travail pour empêcher les utilisateurs d'accéder à leurs postes de travail distants pendant que vous les préparez. Si un pool de postes de travail n'est plus nécessaire, vous pouvez utiliser la fonction de désactivation pour le désactiver sans avoir à supprimer sa définition dans View.

Procédure

1 Dans View Administrator, sélectionnez **Catalogue > Pools de postes de travail**.

2 Sélectionnez un pool de postes de travail et modifiez l'état du pool.

Option	Action
Disable the pool (Désactiver le pool)	Sélectionnez **Désactiver le pool de postes de travail** dans le menu déroulant **État**.
Enable the pool (Activer le pool)	Sélectionnez **Activer le pool de postes de travail** dans le menu déroulant **État**.

3 Cliquez sur **OK**.

Désactiver ou activer le provisionnement dans un pool de postes de travail automatisé

Lorsque vous désactivez le provisionnement dans un pool de postes de travail automatisé, View cesse de provisionner de nouvelles machines au pool. Après avoir désactivé l'approvisionnement, vous pouvez l'activer de nouveau.

Avant de modifier la configuration d'un pool de postes de travail, vous pouvez désactiver le provisionnement pour vous assurer qu'aucune nouvelle machine ne sera créée avec l'ancienne configuration. Vous pouvez également désactiver le provisionnement pour empêcher View d'utiliser un stockage supplémentaire lorsqu'un pool occupe presque tout l'espace disponible.

Lorsque le provisionnement est désactivé dans un pool de clone lié, View cesse de provisionner de nouvelles machines et de personnaliser les machines suite à une recomposition ou à un rééquilibrage.

Procédure

1 Dans View Administrator, sélectionnez **Catalogue > Pools de postes de travail**.

2 Sélectionnez un pool de postes de travail et modifiez l'état du pool.

Option	Action
Disable provisioning (Désactiver l'approvisionnement)	Sélectionnez **Désactiver le provisionnement** dans le menu déroulant **État**.
Activer l'approvisionnement	Sélectionnez **Activer l'approvisionnement** dans le menu déroulant **État**.

3 Cliquez sur **OK**.

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 bande passante utilisée par le contenu Adobe Flash sur des postes de travail distants. Cette réduction peut améliorer l'expérience globale des recherche et rendre d'autres applications exécutées sur le poste de travail distant plus réactives.

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 203.

Procédure

1 Dans View Administrator, sélectionnez **Catalogue > Pools de postes de travail**.

2 Sélectionnez un pool de postes de travail et cliquez sur **Modifier**.

3 Dans l'onglet **Paramètres du pool de postes de travail**, sélectionnez un mode de qualité dans le menu **Qualité Adobe Fash** et un mode de limitation dans le menu **Limitation d'Adobe Flash**

4 Cliquez sur **OK**.

Remarque Les paramètres de réduction de bande passante d'Adobe Flash ne s'appliquent pas tant qu'Horizon Client ne s'est pas reconnecté au poste de travail distant.

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 10-3 montre les paramètres de qualité du rendu Adobe Flash disponibles.

Tableau 10-3. Paramètres de qualité d'Adobe Flash

Paramètre de qualité	Description
Ne pas contrôler	La qualité est déterminée par les paramètres de page Web.
Basse	Ce paramètre se traduit par les meilleures économies de bande passante.
Moyenne	Ce paramètre se traduit par des économies de bande passante modérées.
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 **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 10-4 montre les paramètres de limitation d'Adobe Flash disponibles.

Tableau 10-4. Paramètres de limitation d'Adobe Flash

Paramètre de limitation	Description
Désactivé	Aucune limitation n'est effectuée. L'intervalle du temporisateur n'est pas modifié.
Classique	L'intervalle du temporisateur est de 100 millisecondes. Ce paramètre correspond au plus petit nombre d'images ignorées.
Modérée	L'intervalle du temporisateur est de 500 millisecondes.
Agressive	L'intervalle du temporisateur est de 2 500 millisecondes. Ce paramètre correspond au plus grand nombre d'images ignorées.

La vitesse audio reste constante quel que soit le paramètre de limitation sélectionné.

Supprimer un pool de postes de travail

Lorsque vous supprimez un pool de postes de travail, les utilisateurs ne peuvent plus lancer de nouveaux postes de travail distants dans le pool.

Selon le type de pool de postes de travail, vous disposez de diverses options pour définir la manière dont View traite les disques persistants, les machines virtuelles complètes de vCenter Server et les sessions actives des utilisateurs.

Par défaut, vous pouvez supprimer un pool de postes de travail même s'il existe des machines de poste de travail dans le pool. View ne vous donne pas d'avertissement. Vous pouvez configurer View pour ne pas autoriser la suppression d'un pool qui contient des machines de poste de travail. Pour plus d'informations, reportez-vous à « Configurer View pour interdire la suppression d'un pool de postes de travail qui contient des machines de poste de travail », page 205. Si vous configurez le paramètre, vous devez supprimer toutes les machines dans un pool de postes de travail avant de pouvoir supprimer le pool.

Avec un pool de postes de travail automatisé de clones instantanés ou de clones liés de View Composer, View 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 risque de mettre les composants View dans un état incohérent.

Procédure

1 Dans View Administrator, sélectionnez **Catalogue > Pools de postes de travail**.

2 Sélectionnez un pool de postes de travail et cliquez sur **Supprimer**.

3 Choisissez la méthode de suppression du pool de postes de travail.

Pool	Options
Pool de postes de travail automatisé de clones instantanés ou de clones liés sans disques persistants.	Aucune option disponible. View supprime toutes les machines virtuelles du disque. Les sessions des utilisateurs sur leur poste de travail distant sont interrompues.
Pool de postes de travail automatisé de clone lié avec disques persistants.	Indiquez s'il convient de détacher ou de supprimer les disques persistants lorsque les machines virtuelles de clone lié sont supprimées. Dans les deux cas, View supprime toutes les machines virtuelles du disque, et les sessions des utilisateurs sur leur poste de travail distant sont interrompues. Si vous détachez un disque persistant, la machine virtuelle de clone lié qui contenait le disque persistant peut être recréée ou le disque persistant peut être attaché à une autre machine virtuelle. 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 version ultérieure.
Pool de postes de travail automatisé de machines virtuelles complètes. **Pool de postes de travail manuel de machines virtuelles vCenter Server.**	Choisissez de conserver ou de supprimer les machines virtuelles dans vCenter Server.
Pool de postes de travail RDS. **Pool de postes de travail automatisé de machines virtuelles complètes.** **Pool de postes de travail manuel.**	Si des utilisateurs sont connectés à leur poste de travail distant, indiquez s'il convient de maintenir actives les sessions des utilisateurs ou de les interrompre. Notez que le Serveur de connexion View n'assure pas le suivi des sessions qui sont maintenues actives.

Lorsque vous supprimez un pool de postes de travail, les comptes d'ordinateur de machines virtuelles de clone lié sont supprimés d'Active Directory. Les comptes d'ordinateur de machines virtuelles complètes sont conservés dans Active Directory. Pour supprimer ces comptes, vous devez les supprimer manuellement d'Active Directory.

Si vous supprimez un pool de postes de travail de clone instantané, View peut nécessiter du temps pour supprimer les machines virtuelles internes de vCenter Server. Ne supprimez pas vCenter Server de View Administrator tant que vous n'avez pas vérifié que toutes les machines virtuelles sont supprimées.

Configurer View pour interdire la suppression d'un pool de postes de travail qui contient des machines de poste de travail

Vous pouvez configurer View pour interdire la suppression d'un pool de postes de travail qui contient des machines de poste de travail. Par défaut, View autorise la suppression de ce type de pool.

Si vous configurez ce paramètre, vous devez supprimer toutes les machines dans un pool de postes de travail avant de pouvoir supprimer le pool.

Prérequis

Pour plus d'informations sur l'utilisation de l'utilitaire ADSI Edit sur votre serveur Windows, consultez le site Web Microsoft TechNet.

Procédure

1 Démarrez l'utilitaire ADSI Edit sur l'hôte du Serveur de connexion View.

2 Dans la boîte de dialogue Paramètres de connexion, sélectionnez **DC=vdi,DC=vmware,DC=int** ou connectez-vous à cet objet.

3 Dans le volet Ordinateur, sélectionnez ou tapez **`localhost:389`** ou le nom de domaine complet du 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**, modifiez l'attribut **pae-NameValuePair** et ajoutez la valeur **cs-disableNonEmptyPoolDelete=1**.

Le nouveau paramètre prend effet immédiatement. Vous n'avez pas à redémarrer le service Serveur de connexion View.

Gestion de postes de travail basés sur une machine virtuelle

Un poste de travail basé sur une machine virtuelle est un poste de travail issu d'un pool de postes de travail automatisé ou d'un pool de poste de travail manuel contenant des machines virtuelles vCenter Server.

Attribuer une machine à un utilisateur

Dans un pool à attribution dédiée, vous pouvez désigner un utilisateur comme propriétaire de la machine virtuelle qui héberge un poste de travail distant. Seul l'utilisateur autorisé peut ouvrir une session et se connecter au poste de travail distant.

View attribue des machines à des utilisateurs dans ces situations.

- Lorsque vous créez un pool de postes de travail et sélectionnez le paramètre **Activer l'affectation automatique**.

  Remarque Si vous sélectionnez **Activer l'affectation automatique**, vous pouvez toujours attribuer manuellement des machines à des utilisateurs.

- Lorsque vous créez un pool automatisé, sélectionnez le paramètre **Spécifier des noms manuellement**, puis fournissez des noms d'utilisateur avec les noms de machine.

Si vous ne sélectionnez aucun de ces paramètres dans un pool à attribution dédiée, les utilisateurs n'ont pas accès aux postes de travail distants. Vous devez attribuer manuellement une machine à chaque utilisateur.

Vous pouvez également utiliser la commande `vdmadmin` pour attribuer des machines à des utilisateurs. Reportez-vous à la section « Attribution de machines dédiées à l'aide de l'option -L », page 293.

Prérequis

- Vérifiez que la machine virtuelle du poste de travail distant appartient à un pool à attribution dédiée. Dans View Administrator, l'attribution du pool de postes de travail s'affiche dans la colonne Pool de postes de travail dans la page Machines.

Procédure

1 Dans View Administrator, sélectionnez **Ressources > Machines**, ou sélectionnez **Catalogue > Pools de postes de travail**, double-cliquez sur un ID de pool, puis cliquez sur l'onglet **Inventaire**.

2 Sélectionnez la machine.

3 Sélectionnez **Affecter un utilisateur** dans le menu déroulant **Plus de commandes**.

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 **Nom** ou **Description**.

5 Sélectionnez le nom d'utilisateur ou de groupe et cliquez sur **OK**.

Annuler l'attribution d'une machine dédiée à un utilisateur

Dans un pool à attribution dédiée, vous pouvez annuler l'attribution d'une machine à un utilisateur.

Vous pouvez également utiliser la commande `vdmadmin` pour annuler l'attribution d'une machine à un utilisateur. Reportez-vous à la section « Attribution de machines dédiées à l'aide de l'option -L », page 293.

Procédure

1 Dans View Administrator, sélectionnez **Ressources > Machines** ou sélectionnez **Catalogue > Pools de postes de travail**, double-cliquez sur un ID de pool, puis cliquez sur l'onglet **Inventaire**.

2 Sélectionnez la machine.

3 Sélectionnez **Supprimer l'affectation d'un utilisateur** dans le menu déroulant **Plus de commandes**.

4 Cliquez sur **OK**.

La machine est disponible et peut être attribuée à un autre utilisateur.

Personnaliser des machines existantes en mode de maintenance

Après avoir créé un pool de postes de travail, vous pouvez personnaliser, modifier ou tester des machines individuelles en les mettant en mode de maintenance. Lorsqu'une machine est en mode de maintenance, les utilisateurs ne peuvent pas accéder au poste de travail de la machine virtuelle.

Vous mettez les machines existantes en mode de maintenance, une à la fois. Vous pouvez supprimer plusieurs machines du mode de maintenance en une seule opération.

Lorsque vous créez un pool de postes de travail, vous pouvez démarrer toutes les machines du pool en mode de maintenance si vous spécifiez les noms des machines manuellement. Pour plus d'informations, reportez-vous à la section « Personnalisation des postes de travail en mode de maintenance » dans le document *Configuration des postes de travail virtuels dans Horizon 7*.

Dans Horizon 7.0, cette fonctionnalité n'est pas prise en charge pour les clones instantanés.

Procédure

1 Dans Horizon Administrator, sélectionnez **Ressources > Machines** ou sélectionnez **Catalogue > Pools de postes de travail**, double-cliquez sur un ID de pool, puis sélectionnez l'onglet **Inventaire**.

2 Sélectionnez une machine.

3 Sélectionnez **Passer en mode de maintenance** dans le menu déroulant **Plus de commandes**.

4 Personnalisez, modifiez ou testez le poste de travail de machine virtuelle.

5 Répétez les étapes Étape 2 à Étape 4 pour toutes les machines virtuelles à personnaliser.

6 Sélectionnez les machines personnalisées, puis **Quitter le mode de maintenance** dans le menu déroulant **Plus de commandes**.

Les postes de travail de machine virtuelle modifiés sont disponibles pour les utilisateurs.

Surveiller l'état d'un poste de travail de machine virtuelle

Vous pouvez rapidement contrôler l'état des postes de travail de machine virtuelle de votre déploiement de View dans le tableau de bord de View Administrator. Par exemple, vous pouvez afficher toutes les machines virtuelles déconnectées ou les machines virtuelles qui sont en mode de maintenance.

Prérequis

Familiarisez-vous avec les états de machines virtuelles. Reportez-vous à la section « État des machines virtuelles vCenter Server », page 208.

Procédure

1 Dans View Administrator, cliquez sur **Tableau de bord**.

2 Dans le volet État des machines, développez un dossier d'état.

Option	Description
Préparation	Répertorie les états de machine lorsque la machine virtuelle est en cours de provisionnement, de suppression ou en mode de maintenance.
Machines problématiques	Répertorie les états d'erreur de machine.
Préparé pour l''utilisation	Répertorie les états de la machine lorsque la machine virtuelle est prête à être utilisée.

3 Recherchez l'état des machines et cliquez sur le nombre affiché sous forme de lien hypertexte situé en regard.

La page Machines affiche toutes les machines virtuelles se trouvant dans l'état sélectionné.

Suivant

Vous pouvez cliquer sur un nom de machine pour voir des détails sur cette dernière ou cliquer sur la flèche Précédent dans View Administrator pour revenir à la page Tableau de bord.

État des machines virtuelles vCenter Server

Les machines virtuelles qui sont gérées par vCenter Server peuvent présenter plusieurs états de fonctionnement et de disponibilité. Dans Horizon Administrator, vous pouvez suivre l'état des machines dans la colonne de droite de la page Machines.

Tableau 10-5 montre l'état opérationnel des postes de travail de machine virtuelle affichés dans Horizon Administrator. Un poste de travail ne peut être que dans un seul état à la fois.

Tableau 10-5. État des machines virtuelles qui sont gérées par vCenter Server

État	Description
Approvisionnement	La machine virtuelle est approvisionnée.
Personnalisation	La machine virtuelle dans un pool automatisé est personnalisée.
Suppression	La machine virtuelle est marquée pour être supprimée. Horizon 7 supprimera bientôt la machine virtuelle.
Attente d'agent	Le Serveur de connexion Horizon attend d'établir la communication avec View Agent ou Horizon Agent sur une machine virtuelle dans un pool manuel.
Mode de maintenance	La machine virtuelle est en mode de maintenance. Les utilisateurs ne peuvent pas ouvrir de session ou utiliser la machine virtuelle.

Tableau 10-5. État des machines virtuelles qui sont gérées par vCenter Server (suite)

État	Description
Démarrage	View Agent ou Horizon 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 l'agent autorise d'autres processus, tels que les services de protocole, à démarrer également.
Agent désactivé	Cet état peut se produire dans deux cas. Premier cas : dans un pool de postes de travail pour lequel le paramètre **Supprimer ou actualiser la machine à la fermeture de session** ou **Supprimer la machine après la fermeture de session** est activé, une session de poste de travail est fermée, mais la machine virtuelle n'est pas encore actualisée ni supprimée. Second cas : le Serveur de connexion View désactive View Agent ou Horizon 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.
Agent inaccessible	Le Serveur de connexion Horizon ne peut pas établir de communication avec View Agent ou Horizon Agent sur une machine virtuelle.
IP non valide	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	Un composant Horizon 7 a été mis à niveau et la machine virtuelle doit être redémarrée pour permettre à View Agent ou Horizon Agent de fonctionner avec le composant mis à niveau.
Échec du protocole	Un protocole d'affichage n'a pas démarré avant l'expiration de la période de démarrage de View Agent ou Horizon Agent. **Remarque** View Administrator peut afficher les machines dont l'état est **Échec du protocole** lorsqu'un protocole a échoué alors que d'autres protocoles 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 machines sont disponibles et les périphériques Horizon Client peuvent y accéder via PCoIP ou RDP.
Échec du domaine	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.
Déjà utilisé	Dans un pool de postes de travail pour lequel le paramètre **Supprimer ou actualiser la machine à la fermeture de session** ou **Supprimer la machine après la fermeture de session** est activé, aucune session n'est active sur la machine virtuelle, mais la session n'a pas été fermée. Cette situation peut se produire si une machine virtuelle s'arrête de façon imprévue ou si l'utilisateur réinitialise la machine pendant une session. Par défaut, lorsqu'une machine virtuelle est dans cet état, Horizon 7 empêche tous les autres périphériques Horizon Client d'accéder au poste de travail.
Erreur de configuration	Le protocole d'affichage comme RDP ou PCoIP n'est pas activé.
Erreur d'approvisionnement	Une erreur s'est produite au cours de l'approvisionnement.
Erreur	Une erreur inconnue s'est produite dans la machine virtuelle.
Utilisateur non affecté connecté	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	Un utilisateur qui n'est pas l'utilisateur autorisé a ouvert une session et est déconnecté d'une machine virtuelle dans un pool à attribution dédiée.
Inconnu	La machine virtuelle est dans un état inconnu.
Approvisionné	La machine virtuelle est hors tension ou interrompue.

Tableau 10-5. État des machines virtuelles qui sont gérées par vCenter Server (suite)

État	Description
Disponible	La machine virtuelle est sous tension et prête pour une connexion. Dans un pool dédié, la machine virtuelle est affectée à un utilisateur et démarre quand l'utilisateur ouvre une session.
Connecté	La machine virtuelle est dans une session active et dispose d'une connexion distante au périphérique Horizon Client.
Déconnecté	La machine virtuelle est dans une session, mais est déconnectée du périphérique Horizon Client.
En cours	La machine virtuelle est dans un état de transition lors d'une opération de maintenance.

Lorsqu'une machine se trouve dans un état particulier, elle peut présenter d'autres conditions. Horizon Administrator affiche ces conditions sous la forme de suffixes à l'état de la machine. Par exemple, Horizon Administrator peut afficher l'état `Customizing (missing) (Personnalisation (manquant))`.

Tableau 10-6 montre ces conditions supplémentaires.

Tableau 10-6. Conditions d'état de la machine

Condition	Description
Missing (Manquant)	La machine virtuelle est manquante dans vCenter Server. Généralement, la machine virtuelle a été supprimée dans vCenter Server, mais la configuration Horizon LDAP dispose toujours d'un enregistrement de la machine.
Task halted (Tâche arrêtée)	Une tâche de clone instantané, telle qu'une image de transfert, ou 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 185 Pour plus d'informations sur les états d'erreur de View Composer, reportez-vous à la section « Erreurs de provisionnement de View Composer » dans le document *Configuration des postes de travail virtuels dans Horizon 7*. La condition `Task halted (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 démarrée. Les machines virtuelles dans le pool qui ne sont pas sélectionnées pour l'opération ne sont pas placées dans la condition `Task halted (Tâche arrêtée)`.

Un état de machine peut présenter deux conditions, `(manquant, tâche arrêtée)`, si une tâche de View Composer a été arrêtée et que la machine virtuelle est absente dans vCenter Server.

Supprimer des postes de travail de machine virtuelle

Lorsque vous supprimez un poste de travail de machine virtuelle, les utilisateurs ne peuvent plus accéder au poste de travail. Un poste de travail de machine virtuelle peut être une machine virtuelle vCenter Server ou un machine virtuelle non gérée.

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 de machine virtuelle supprimés.

Avec des clones instantanés et des machines virtuelles 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 de machine virtuelle avec View Administrator. Cette action risque de mettre les composants View dans un état incohérent.

Procédure

1 Dans View Administrator, sélectionnez **Ressources > Machines**.

2 Sélectionnez l'onglet **Machines virtuelles vCenter** ou l'onglet **Autres**.

3 Sélectionnez une ou plusieurs machines et cliquez sur **Supprimer**.

4 Choisissez le mode de suppression des postes de travail de machine virtuelle.

Option	Description
Pool that contains full virtual-machine desktops (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 View Composer avec disques persistants	Indiquez s'il convient de détacher ou de supprimer les disques persistants lorsque les postes de travail de machine virtuelle sont supprimés. Dans les deux cas, vCenter Server supprime les machines virtuelles de clone lié du disque. Les utilisateurs des sessions actuellement actives sont déconnectés de leurs postes de travail distants. Si vous détachez un disque persistant, la machine virtuelle de clone lié qui contenait le disque persistant peut être recréée ou le disque persistant peut être attaché à une autre machine virtuelle. 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 version ultérieure.
Pool de clone instantané et pool de clone lié View Composer sans disques persistants	vCenter Server supprime les machines virtuelles de clone lié du disque. Les utilisateurs des sessions actuellement actives sont déconnectés de leurs postes de travail distants.

Lorsque vous supprimez des postes de travail de machine virtuelle, les comptes d'ordinateur de machine virtuelle 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.

Récupérer des postes de travail de clone instantané

Lorsqu'un poste de travail de clone instantané est dans un état d'erreur, vous avez la possibilité de le récupérer. Le poste de travail est recréé à partir de l'image de base actuelle.

Procédure

1 Dans View Administrator, sélectionnez **Catalogue > Pools de postes de travail**, double-cliquez sur l'ID d'un pool, puis cliquez sur l'onglet **Inventaire**.

2 Sélectionnez une ou plusieurs machines et cliquez sur **Récupérer**.

Gestion de machines non gérées

Dans View Administrator, vous pouvez ajouter des machines non gérées à des pools de postes de travail manuels et en supprimer. Vous pouvez également supprimer de View des machines enregistrées. Des machines non gérées sont des ordinateurs physiques et des machines virtuelles qui ne sont pas gérés par vCenter Server.

Pour plus d'informations sur la suppression d'un pool de postes de travail contenant des machines non gérées, reportez-vous à « Supprimer un pool de postes de travail », page 204.

Lorsque vous reconfigurez un paramètre qui affecte une machine non gérée, la prise en compte du nouveau paramètre peut prendre jusqu'à 10 minutes. Par exemple, si vous modifiez le mode de sécurité des messages dans Paramètres généraux ou le paramètre **Fermeture de session automatique après la déconnexion** pour un pool, View peut nécessiter jusqu'à 10 minutes pour reconfigurer les machines non gérées affectées.

Remarque Les hôtes RDS sont également des machines non gérées, car ils ne sont pas générés à partir d'une machine virtuelle parente ou d'un modèle, et ne sont pas gérés par vCenter Server. Les hôtes RDS prennent en charge les applications et les postes de travail basés sur une session et sont considérés comme faisant partie d'une catégorie distincte. Reportez-vous à la section « Gestion des hôtes RDS », page 224.

Ajouter une machine non gérée à un pool manuel

Vous pouvez augmenter la taille d'un pool de postes de travail manuel en y ajoutant des machines non gérées.

Prérequis

Vérifiez qu'Horizon Agent est installé sur la machine non gérée. Pour plus d'informations sur la préparation d'une machine non gérée, reportez-vous à la section « Installer Horizon Agent sur une machine non gérée » dans le document *Configuration des postes de travail virtuels dans Horizon 7*.

Procédure

1 Dans Horizon Administrator, sélectionnez **Catalogue > Pools de postes de travail**.

2 Double-cliquez sur l'ID du pool manuel.

3 Sous l'onglet **Inventaire**, cliquez sur **Ajouter**.

4 Sélectionnez les machines non gérées dans la fenêtre Ajouter des postes de travail et cliquez sur **OK**.

Les machines non gérées sont ajoutées au pool.

Supprimer une machine non gérée d'un pool de postes de travail manuel

Vous pouvez réduire la taille d'un pool de postes de travail manuel en supprimant les machines non gérées du pool.

Procédure

1 Dans View Administrator, sélectionnez **Catalogue > Pools de postes de travail**.

2 Double-cliquez sur l'ID du pool manuel.

3 Sélectionnez l'onglet **Inventaire**.

4 Sélectionnez les machines non gérées à supprimer.

5 Cliquez sur **Supprimer**.

6 Si des utilisateurs sont connectés aux postes de travail basés sur une machine non gérée, indiquez s'il convient de mettre fin aux sessions ou de les laisser actives.

Option	Description
Laisser active	Les sessions actives le resteront jusqu'à ce que l'utilisateur ferme sa session. Le Serveur de connexion View ne garde pas de trace de ces sessions.
Mettre fin	Les sessions actives sont terminées immédiatement.

7 Cliquez sur **OK**.

Les machines non gérées sont supprimées du pool.

Supprimer des machines inscrites de View

Si vous ne prévoyez pas de réutiliser une machine inscrite, vous pouvez la supprimer de View.

Il existe deux types de machines inscrites dans View : Hôtes RDS et Autres. Les machines non gérées appartiennent à la catégorie Autres. Des machines non gérées sont des ordinateurs physiques et des machines virtuelles qui ne sont pas gérés par vCenter Server. Elles servent à former des pools de postes de travail manuels qui ne contiennent pas de machines virtuelles vCenter Server.

Dès qu'une machine inscrite est supprimée, elle devient indisponible dans View. Pour rendre la machine à nouveau disponible, vous devez réinstaller Horizon Agent.

Prérequis

Vérifiez que les machines inscrites que vous souhaitez supprimer ne sont pas utilisées dans un pool de postes de travail.

Procédure

1 Dans View Administrator, sélectionnez **Configuration de View > Machines inscrites**.

2 Cliquez sur l'onglet **Autres**.

3 Sélectionnez une ou plusieurs machines et cliquez sur **Supprimer**.

Vous ne pouvez sélectionner que les machines qui ne sont pas utilisées par un pool de postes de travail.

4 Cliquez sur **OK** pour confirmer.

État des machines non gérées

Les machines non gérées, qui sont des ordinateurs physiques ou des machines virtuelles non gérés par vCenter Server, peuvent avoir différents états de fonctionnement et de disponibilité. Dans View Administrator, vous pouvez effectuer le suivi des machines non gérées dans la colonne de droite de la page Machines dans l'onglet **Autres**.

Tableau 10-7 présente l'état opérationnel des machines non gérées affichées dans View Administrator. Une machine ne peut être que dans un seul état à la fois.

Tableau 10-7. État des machines non gérées

État	Description
Démarrage	View Agent ou Horizon Agent a démarré sur la machine, mais d'autres services requis, comme le protocole d'affichage, sont toujours en cours de démarrage. La période de démarrage de l'agent autorise d'autres processus, tels que les services de protocole, à démarrer également.
Validation	Cet état se produit lorsque le Serveur de connexion View détecte la machine pour la première fois, en général après le démarrage ou le redémarrage du Serveur de connexion View, et avant la première communication réussie avec View Agent ou Horizon Agent sur la machine. Cet état est généralement temporaire. Cet état n'est pas le même que l'état Agent inaccessible, qui indique un problème de communication.
Agent désactivé	Cet état peut se produire si le Serveur de connexion View désactive View Agent ou Horizon Agent. Il empêche le démarrage d'une nouvelle session de poste de travail sur la machine.
Agent inaccessible	Le Serveur de connexion View ne parvient pas à établir de communication avec View Agent ou Horizon Agent sur la machine. La machine est peut-être hors tension.
IP non valide	Le paramètre de registre Masque de sous-réseau est configuré sur la machine et aucun adaptateur réseau actif ne dispose d'une d'adresse IP dans la plage configurée.
L'agent doit redémarrer	Un composant View a été mis à niveau et la machine doit être redémarrée pour permettre à View Agent ou Horizon Agent de fonctionner avec le composant mis à niveau.
Échec du protocole	Un protocole d'affichage n'a pas démarré avant l'expiration de la période de démarrage de View Agent ou Horizon Agent. **Remarque** View Administrator peut afficher les machines dont l'état est **Échec du protocole** lorsqu'un protocole a échoué alors que d'autres protocoles 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 machines sont disponibles et les périphériques Horizon Client peuvent y accéder via PCoIP ou RDP.
Échec du domaine	La machine a rencontré un problème en tentant d'atteindre le domaine. Le serveur de domaine n'était pas accessible ou l'authentification de domaine a échoué.
Erreur de configuration	Le protocole d'affichage tel que RDP ou autre protocole n'est pas activé.
Utilisateur non affecté connecté	Un utilisateur qui n'est pas l'utilisateur attribué a ouvert une session sur une machine d'un pool à attribution dédiée. Par exemple, cet état peut se présenter si un administrateur ouvre une session sur la machine non gérée sans utiliser Horizon Client.
Utilisateur non affecté déconnecté	Un utilisateur qui n'est pas l'utilisateur attribué a ouvert une session sur une machine d'un pool à attribution dédiée et a été déconnecté.
Inconnu	L'état de la machine est inconnu.
Disponible	L'ordinateur faisant office de source de poste de travail est sous tension et le poste de travail est prêt pour une connexion. Dans un pool dédié, le poste de travail est affecté à un utilisateur. Le poste de travail démarre quand l'utilisateur ouvre une session.
Connecté	Le poste de travail a une session ouverte et dispose d'une connexion à distance à un périphérique Horizon Client.
Déconnecté	Le poste de travail a une session ouverte, mais il est déconnecté du périphérique Horizon Client.

Gérer des sessions d'applications et de postes de travail publiés

Lorsqu'un utilisateur lance une application ou un poste de travail publié, une session se crée. Vous pouvez déconnecter et fermer des sessions, envoyer des messages aux clients, réinitialiser et redémarrer des machines virtuelles.

Procédure

1 Dans Horizon Administrator, accédez à l'emplacement dans lequel sont affichées les informations de session.

Type de session	Navigation
Sessions de postes de travail distants	Sélectionnez **Catalogue > Pools de postes de travail**, double-cliquez sur l'ID d'un pool, puis cliquez sur l'onglet **Sessions**.
Sessions d'applications et de postes de travail distants	Sélectionnez **Contrôle > Sessions**.
Sessions associées à un utilisateur ou à groupe d'utilisateurs	■ Sélectionnez **Utilisateurs et groupes**. ■ Double-cliquez sur un nom d'utilisateur ou de groupe d'utilisateurs. ■ Cliquez sur l'onglet **Sessions**.

2 Sélectionnez une session.

Pour envoyer un message aux utilisateurs, vous pouvez sélectionner plusieurs sessions. Vous pouvez effectuer les autres opérations sur une seule session à la fois.

3 Indiquez si vous souhaitez déconnecter, fermer une session, envoyer un message ou réinitialiser une machine virtuelle.

Option	Description
Déconnecter la session	Déconnecte l'utilisateur de la session.
Fermer la session	Ferme la session de l'utilisateur. Les données qui ne sont pas enregistrées seront perdues.
Envoyer un message	Envoyez un message à Horizon Client. Vous pouvez nommer le message **Infos**, **Avertissement** ou **Erreur**.

4 Cliquez sur **OK**.

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 machines, 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 machines gérées par plusieurs instances du Serveur de connexion View ou groupes d'instances du Serveur de connexion View répliquées. Vous pouvez exporter le tableau Machines 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 de valeurs séparées par des virgules (CSV). 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 **Ressources > Machines** pour afficher le tableau des machines.

2 Cliquez sur l'icône Exporter dans le coin supérieur droit du tableau.

   Lorsque vous pointez sur l'icône, l'info-bulle `Exporter le contenu du tableau` s'affiche.

3 Tapez un nom de fichier pour le fichier CSV dans la boîte de dialogue 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 **Enregistrer**.

Suivant

Ouvrez un tableur ou un autre outil pour afficher le fichier CSV.

Gestion de pools d'applications, de batteries de serveurs et d'hôtes RDS 11

Dans Horizon Administrator, vous pouvez effectuer des opérations de gestion comme la configuration ou la suppression de pools de postes de travail, de batteries de serveurs ou d'hôtes RDS.

Ce chapitre aborde les rubriques suivantes :

Gestion de pools d'applications

Vous pouvez ajouter, modifier, supprimer ou autoriser des pools d'applications dans Horizon Administrator.

Pour ajouter un pool d'applications, reportez-vous à la section « Création de pools d'applications » dans le document *Configuration d'applications et de postes de travail publiés dans Horizon 7*. Pour autoriser un pool d'applications, reportez-vous à la section « Autorisation d'utilisateurs et de groupes » dans le document *Configuration d'applications et de postes de travail publiés dans Horizon 7*.

Modifier un pool d'applications

Vous pouvez modifier un pool d'applications existant pour configurer des paramètres comme le nom d'affichage, la version, l'éditeur, le chemin d'accès, le dossier de démarrage, les paramètres et la description. Vous ne pouvez pas modifier l'ID ou le groupe d'accès d'un pool d'applications.

Si vous devez vous assurer que le Serveur de connexion View lance l'application uniquement sur des hôtes RDS disposant de ressources suffisantes pour exécuter l'application, reportez-vous à la section « Configurer une règle anti-affinité pour un pool d'applications », page 235.

Prérequis

Familiarisez-vous avec les paramètres d'un pool d'applications. Reportez-vous à la section « Création de pools d'applications » dans le document *Configuration d'applications et de postes de travail publiés dans Horizon 7*.

Procédure

1 Dans Horizon Administrator, sélectionnez **Catalogue > Pools d'applications**.

2 Sélectionnez un pool et cliquez sur **Modifier**.

3 Apportez les changements aux paramètres du pool.

4 Cliquez sur **OK**.

Supprimer un pool d'applications

Lorsque vous supprimez un pool d'applications, les utilisateurs ne peuvent plus lancer l'application dans le pool.

Vous pouvez supprimer un pool d'applications, même si les utilisateurs accèdent actuellement à l'application. Dès que les utilisateurs referment l'application, ils ne peuvent plus y accéder.

Procédure

1 Dans Horizon Administrator, sélectionnez **Catalogue > Pools d'applications**.

2 Sélectionnez un ou plusieurs pools d'applications, puis cliquez sur **Supprimer**.

3 Cliquez sur **OK** pour confirmer.

Gestion de batteries de serveurs

Dans Horizon Administrator, vous pouvez ajouter, modifier, supprimer, activer et désactiver des batteries de serveurs.

Pour ajouter une batterie de serveurs, reportez-vous à la section « Création de batteries de serveurs » dans le document *Configuration d'applications et de postes de travail publiés dans Horizon 7*. Pour plus d'informations sur les groupes d'accès, reportez-vous à Chapitre 6, « Configuration d'administration déléguée basée sur des rôles », page 111.

Après la création d'une batterie de serveurs, vous pouvez ajouter ou supprimer des hôtes RDS pour prendre charge plus ou moins d'utilisateurs.

Modifier une batterie de serveurs

Pour une batterie de serveurs existante, vous pouvez apporter des modifications aux paramètres de configuration.

Prérequis

Familiarisez-vous avec les paramètres d'une batterie de serveurs. Reportez-vous à la section « Création de batteries de serveurs » dans le document *Configuration d'applications et de postes de travail publiés dans Horizon 7*.

Procédure

1 Dans Horizon Administrator, sélectionnez **Ressources > Batteries de serveurs**.

2 Sélectionnez une batterie de serveurs et cliquez sur **Modifier**.

3 Modifiez les paramètres de la batterie de serveurs.

4 Cliquez sur **OK**.

Supprimer une batterie de serveurs

Vous pouvez supprimer une batterie de serveurs si vous n'en avez plus besoin ou si vous souhaitez en créer une nouvelle avec des hôtes RDS différents. Vous ne pouvez supprimer une batterie de serveurs que si elle n'est pas associée à un pool de postes de travail RDS ou à un pool d'applications.

Prérequis

Vérifiez que la batterie de serveurs n'est pas associée à un pool de postes de travail RDS ou à un pool d'applications.

Procédure

1 Dans Horizon Administrator, sélectionnez **Ressources > Batteries de serveurs**.

2 Sélectionnez une ou plusieurs batteries de serveurs et cliquez sur **Supprimer**.

3 Cliquez sur **OK** pour confirmer.

Désactiver ou activer une batterie de serveurs

Lorsque vous désactivez une batterie de serveurs, les utilisateurs ne peuvent plus lancer de postes de travail ou d'applications RDS à partir des pools de postes de travail RDS et des pools d'applications associés à la batterie de serveurs. Les utilisateurs peuvent continuer à utiliser les applications et les postes de travail RDS qui sont actuellement ouverts.

Vous pouvez désactiver une batterie de serveurs si vous prévoyez d'effectuer de la maintenance sur ses hôtes RDS ou sur les pools de postes de travail et d'applications RDS associés à la batterie. Une fois la batterie de serveurs désactivée, certains utilisateurs peuvent continuer à utiliser les postes de travail ou les applications RDS qu'ils ont ouverts avant sa désactivation.

Procédure

1 Dans Horizon Administrator, sélectionnez **Ressources > Batteries de serveurs**.

2 Sélectionnez une ou plusieurs batteries de serveurs, et cliquez sur **Plus de commandes**.

3 Cliquez sur **Activer** ou **Désactiver**.

4 Cliquez sur **OK** pour confirmer.

L'état des pools de postes de travail et des pools d'applications RDS associés à la batterie de serveurs est désormais Non disponible. Vous pouvez afficher l'état des pools en sélectionnant **Catalogue > Pools de postes de travail** ou **Catalogue > Pools d'applications**.

Recomposer une batterie de serveurs de clone lié automatisée

Avec l'opération de recomposition de View Composer, vous pouvez mettre à jour l'image de machine de tous les hôtes RDS dans une batterie de serveurs de clone lié automatisée. Vous pouvez mettre à jour les paramètres matériels ou le logiciel de la machine virtuelle parente et exécuter l'opération de recomposition pour que les modifications soient propagées à tous les hôtes RDS dans la batterie de serveurs.

Vous pouvez apporter des modifications à la machine virtuelle parente sans affecter les clones liés d'hôte RDS, car les clones sont liés à un réplica du parent. L'opération de recomposition supprime l'ancien réplica et en crée un nouveau auxquels se lient les clones. La recomposition crée des clones liés, qui utilisent en général moins de stockage, car la taille des fichiers de disque de clones liés croît avec le temps.

Vous pouvez recomposer une batterie de serveurs automatisée mais pas des hôtes RDS individuels dans la batterie de serveurs. Vous ne pouvez pas recomposer de clones liés sur un matériel avec une version inférieure à la version actuelle.

Si possible, planifiez des opérations de recomposition pendant les heures creuses, car l'opération peut prendre du temps.

Prérequis

- Vérifiez que vous disposez d'un snapshot d'une machine virtuelle parente. Vous devez spécifier un snapshot lorsque vous recomposez. Le snapshot peut se trouver sur la machine virtuelle parente actuelle ou sur une autre.
- Décidez à quel moment planifier une opération de recomposition. Par défaut, View Composer démarre l'opération immédiatement.

  Vous ne pouvez planifier qu'une seule opération de recomposition à la fois pour une batterie de serveurs. Vous pouvez recomposer plusieurs batteries de serveurs simultanément.
- Décidez de forcer tous les utilisateurs à fermer leur session dès que l'opération de recomposition commence ou d'attendre que chaque utilisateur ferme sa session avant de recomposer la machine de cet utilisateur.

  Si vous forcez les utilisateurs à fermer leurs sessions, Horizon 7 informe les utilisateurs avant qu'ils soient déconnectés et les autorise à fermer leurs applications et leur session.
- Décidez d'arrêter l'apprivisionnement à la première erreur. Si vous sélectionnez cette option et qu'une erreur se produit lorsque View Composer provisionne un clone lié, le provisionnement s'arrête. 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 **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 le provisionnement est activé. Lorsque le provisionnement est désactivé, Horizon 7 empêche la personnalisation des machines après leur recomposition.
- Si votre déploiement comporte des instances répliquées du Serveur de connexion, vérifiez que toutes les instances ont la même version.

Procédure

1 Dans Horizon Administrator, sélectionnez **Ressources > Batteries de serveurs**.

2 Double-cliquez sur l'ID de pool de la batterie de serveurs que vous voulez recomposer.

3 Cliquez sur **Recomposer**.

4 (Facultatif) Cliquez sur **Modifier** pour modifier la machine virtuelle parente.

  La nouvelle machine virtuelle parente doit exécuter la même version du système d'exploitation que la machine virtuelle parente actuelle.

5 Sélectionnez un snapshot.

6 (Facultatif) Cliquez sur Détails du snapshot pour afficher des détails sur le snapshot.

7 Cliquez sur **Suivant**.

8 (Facultatif) Planifiez une heure de début.

  L'heure actuelle est remplie par défaut.

9 (Facultatif) Spécifiez si vous voulez forcer les utilisateurs à fermer leur session ou attendre que les utilisateurs ferment leur session.

  L'option pour forcer les utilisateurs à fermer leur session est sélectionnée par défaut.

10 (Facultatif) Spécifiez si vous voulez arrêter le provisionnement à la première erreur.

Cette option est sélectionnée par défaut.

11 Cliquez sur **Suivant**.

La page Prêt à terminer s'affiche.

12 (Facultatif) Cliquez sur **Afficher les détails** pour afficher des détails de l'opération de recomposition.

13 Cliquez sur **Terminer**.

Dans vCenter Server, vous pouvez surveiller la progression de l'opération de recomposition sur les machines virtuelles de clone lié.

Remarque Lors de l'opération de recomposition, View Composer exécute de nouveau Sysprep sur les clones liés. De nouveaux SID et des GUID tiers peuvent être générés pour les machines virtuelles recomposées. Pour plus d'informations, reportez-vous à la section « Recomposition de clones liés personnalisés avec Sysprep » dans le document *Configuration des postes de travail virtuels dans Horizon 7*.

Planifier la maintenance d'une batterie de serveurs de clone instantané automatisée

Avec l'opération de maintenance, vous pouvez planifier une maintenance périodique ou immédiate de tous les hôtes RDS dans une batterie de serveurs de clone instantané automatisée. Lors de chaque cycle de maintenance, tous les hôtes RDS sont actualisés à partir de la machine virtuelle parente.

Vous pouvez apporter des modifications à la machine virtuelle parente sans affecter les clones instantanés d'hôte RDS, car le snapshot de la VM parente actuelle est utilisé pour la maintenance. Les clones instantanés créés dans la batterie de serveurs automatisée utilisent les informations dans la VM parente pour leur configuration système.

Vous pouvez planifier la maintenance sur une batterie de serveurs automatisée, mais pas sur des hôtes RDS individuels dans la batterie de serveurs.

Si possible, planifiez les opérations de maintenance pendant les heures creuses pour vous assurer que tous les hôtes RDS ont terminé la maintenance et qu'ils sont disponibles pendant les heures de pointe.

Prérequis

- Décidez à quel moment planifier une opération de maintenance. Par défaut, le Serveur de connexion démarre l'opération immédiatement.

  Vous pouvez planifier une maintenance immédiate, une maintenance récurrente ou les deux pour une batterie de serveurs. Vous pouvez planifier des opérations de maintenance sur plusieurs batteries de serveurs en même temps.

- Décidez de forcer tous les utilisateurs à fermer leur session lorsque l'opération de maintenance commence ou d'attendre que chaque utilisateur ferme sa session avant d'actualiser la machine de cet utilisateur.

  Si vous forcez les utilisateurs à fermer leurs sessions, Horizon 7 informe les utilisateurs avant qu'ils soient déconnectés et les autorise à fermer leurs applications et leur session.

- Choisissez la taille minimale de la batterie de serveurs. La taille minimale de la batterie de serveurs est le nombre d'hôtes RDS qui restent disponibles tout le temps afin de permettre aux utilisateurs de continuer à utiliser la batterie de serveurs. Par exemple, si la taille de la batterie de serveurs est de dix et que la taille minimale de la batterie de serveurs est de deux, la maintenance est exécutée sur huit hôtes RDS. Dès qu'un hôte RDS redevient disponible, les hôtes restants partent en maintenance. Tous les hôtes RDS sont gérés individuellement. Ainsi, dès qu'un hôte devient disponible, l'un des hôtes restants est mis en mode de maintenance.

Toutefois, si vous planifiez une maintenance immédiate, tous les hôtes RDS dans la batterie de serveurs sont mis en mode de maintenance.

Tous les hôtes RDS sont également soumis à une stratégie et ils attendent la fermeture de session ou ils forcent les utilisateurs à fermer la session en fonction de la stratégie configurée.

- Décidez d'arrêter l'apprivisionnement à la première erreur. Si vous sélectionnez cette option et qu'une erreur se produit lorsque le Serveur de connexion provisionne un clone instantané, le provisionnement s'arrête. 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 **Arrêter à la première erreur** n'affecte pas la personnalisation. Si une erreur de personnalisation se produit sur un clone instantané, le provisionnement et la personnalisation des autres clones continuent.

- Vérifiez que le provisionnement est activé. Lorsque le provisionnement est désactivé, Horizon 7 empêche la personnalisation des machines après leur actualisation.

- Si votre déploiement comporte des instances répliquées du Serveur de connexion, vérifiez que toutes les instances ont la même version.

Procédure

1 Dans Horizon Administrator, sélectionnez **Ressources > Batteries de serveurs**.

2 Double-cliquez sur l'ID de pool de la batterie de serveurs pour laquelle vous voulez planifier une maintenance.

3 Cliquez sur **Maintenance > Planifier**.

4 Dans l'assistant Replanifier la maintenance récurrente, choisissez un mode de maintenance.

◆

Option	Action
Récurrent	Planifie une maintenance périodique de tous les serveurs d'hôte RDS dans une batterie de serveurs. ■ Sélectionnez une date et une heure pour la maintenance. ■ Sélectionnez une période de maintenance. Vous pouvez sélectionner des périodes de maintenance quotidienne, mensuelle ou hebdomadaire. ■ Sélectionnez un intervalle de répétition en jours pour l'opération de maintenance. Si une maintenance immédiate est planifiée sur une batterie de serveurs, la date de la maintenance immédiate devient la date effective des maintenances récurrentes. Si vous annulez la maintenance immédiate, la date actuelle devient la date effective des maintenances récurrentes.
Immédiate	Planifie une maintenance immédiate de tous les serveurs d'hôte RDS dans une batterie de serveurs. La maintenance immédiate crée une planification de maintenance unique pour une maintenance qui a lieu immédiatement ou dans un futur proche. Utilisez la maintenance immédiate pour actualiser la batterie de serveurs à partir d'un nouveau snapshot ou d'une nouvelle image de VM parente lorsque vous voulez appliquer des correctifs de sécurité urgents. Sélectionnez une configuration de maintenance immédiate. ■ Sélectionnez **Démarrer maintenant** pour démarrer l'opération de maintenance immédiatement. ■ Sélectionnez **Début à** pour démarrer l'opération de maintenance à une date et une heure proches. Entrez la date et l'heure locale du navigateur Web. **Remarque** La maintenance récurrente sera suspendue jusqu'à ce que la maintenance immédiate se termine.

5 Cliquez sur **Suivant**.

6 (Facultatif) Cliquez sur **Modifier** pour modifier la machine virtuelle parente.

7 Sélectionnez un snapshot.

Vous ne pouvez pas sélectionner un snapshot différent sauf si vous décochez la case **Utiliser l'image de la machine virtuelle parente actuelle**.

8 (Facultatif) Cliquez sur **Détails du snapshot** pour afficher des détails sur le snapshot.

9 Cliquez sur **Suivant**.

10 (Facultatif) Spécifiez si vous voulez forcer les utilisateurs à fermer leur session ou attendre que les utilisateurs ferment leur session.

L'option pour forcer les utilisateurs à fermer leur session est sélectionnée par défaut.

11 (Facultatif) Spécifiez si vous voulez arrêter le provisionnement à la première erreur.

Cette option est sélectionnée par défaut.

12 Cliquez sur **Suivant**.

La page Prêt à terminer s'affiche.

13 Cliquez sur **Terminer**.

Gestion des hôtes RDS

Vous pouvez gérer des hôtes RDS que vous configurez manuellement et des hôtes RDS qui sont créés automatiquement lorsque vous ajoutez une batterie de serveurs automatisée.

Lorsque vous configurez manuellement un hôte RDS, il s'inscrit automatiquement sur le Serveur de connexion Horizon. Vous ne pouvez pas inscrire manuellement un hôte RDS sur le Serveur de connexion. Reportez-vous à la section « Configuration d'hôtes de session de poste de travail distant » dans le document *Configuration d'applications et de postes de travail publiés dans Horizon 7*. Pour un hôte RDS que vous configurez manuellement, vous pouvez exécuter les tâches de gestion suivantes :

- Modifier l'hôte RDS.
- Ajouter l'hôte RDS à une batterie de serveurs manuelle.
- Supprimer l'hôte RDS d'une batterie de serveurs.
- Activer l'hôte RDS.
- Désactiver l'hôte RDS.

Pour un hôte RDS qui est créé automatiquement lorsque vous ajoutez une batterie de serveurs automatisée, vous pouvez effectuer les tâches de gestion suivantes :

- Supprimer l'hôte RDS d'une batterie de serveurs.
- Activer l'hôte RDS.
- Désactiver l'hôte RDS.

Modifier un hôte RDS

Vous pouvez modifier le nombre de connexions qu'un hôte RDS peut prendre en charge. Ce paramètre est le seul que vous pouvez modifier. La valeur par défaut est 150. Vous pouvez la définir sur n'importe quel nombre positif ou sur Illimité.

Vous ne pouvez modifier qu'un hôte RDS que vous configurez manuellement, mais pas un hôte RDS se trouvant dans une batterie de serveurs automatisée.

Procédure

1 Dans View Administrator, sélectionnez **Configuration de View > Machines inscrites**.

2 Sélectionnez un hôte RDS et cliquez sur **Modifier**.

3 Spécifiez une valeur pour le paramètre **Nombre de connexions**.

4 Cliquez sur **OK**.

Ajouter un hôte RDS à une batterie de serveurs manuelle

Vous pouvez ajouter un hôte RDS que vous configurez manuellement à une batterie de serveurs manuelle pour augmenter l'échelle de la batterie de serveurs ou pour d'autres raisons. Vous ne pouvez ajouter que des hôtes RDS à une batterie de serveurs manuelle.

Procédure

1 Dans View Administrator, sélectionnez **Ressources > Batteries de serveurs**.

2 Double-cliquez sur l'ID de pool de la batterie de serveurs.

3 Sélectionnez l'onglet **Hôtes RDS**.

4 Sélectionnez un ou plusieurs hôtes RDS.

5 Cliquez sur **OK**.

Supprimer un hôte RDS d'une batterie de serveurs

Vous pouvez supprimer un hôte RDS d'une batterie de serveurs manuelle pour réduire l'échelle de cette dernière, pour effectuer une maintenance sur l'hôte RDS ou pour d'autres raisons. Nous vous recommandons de désactiver l'hôte RDS et de vous assurer que les utilisateurs ont fermé les sessions actives avant de supprimer un hôte d'une batterie de serveurs.

Si des utilisateurs ont de sessions d'application ou de poste de travail ouvertes sur les hôtes que vous supprimez, les sessions restent actives, mais View ne peut plus en assurer le suivi. Un utilisateur qui se déconnecte d'une session ne pourra plus s'y reconnecter, et toutes les données non enregistrées risquent d'être perdues.

Vous pouvez également supprimer un hôte RDS d'une batterie de serveurs automatisée. Vous pouvez effectuer cette opération si l'hôte RDS se trouve dans un état d'erreur irrécupérable. View Composer crée automatiquement un nouvel hôte RDS pour remplacer celui que vous supprimez.

Procédure

1 Dans View Administrator, sélectionnez **Ressources > Batteries de serveurs**.

2 Double-cliquez sur l'ID de pool.

3 Sélectionnez l'onglet **Hôtes RDS**.

4 Sélectionnez un ou plusieurs hôtes RDS.

5 Cliquez sur **Supprimer de la batterie de serveurs**.

6 Cliquez sur **OK**.

Supprimer un hôte RDS de Horizon 7

Vous pouvez supprimer de Horizon 7 un hôte RDS que vous configurez manuellement et que vous prévoyez de ne plus utiliser. L'hôte RDS ne doit pas se trouver dans une batterie de serveurs manuelle.

Prérequis

Vérifiez que l'hôte RDS n'appartient pas à une batterie de serveurs.

Procédure

1 Dans Horizon Administrator, sélectionnez **Configuration de View > Machines inscrites**.

2 Sélectionnez un hôte RDS et cliquez sur **Supprimer**.

3 Cliquez sur **OK**.

Pour réutiliser un hôte RDS que vous avez supprimé, vous devez réinstaller Horizon Agent. Reportez-vous à la section « Configuration d'hôtes de session de poste de travail distant » dans le document *Configuration d'applications et de postes de travail publiés dans Horizon 7*.

Désactiver ou activer un hôte RDS

Lorsque vous désactivez un hôte RDS, View ne l'utilise plus pour héberger de nouveaux postes de travail ou de nouvelles applications RDS. Les utilisateurs peuvent continuer à utiliser les applications et les postes de travail RDS qui sont actuellement ouverts.

Procédure

1 Dans View Administrator, sélectionnez **Ressources > Batteries de serveurs**.

2 Double-cliquez sur l'ID de pool d'une batterie de serveurs.

3 Sélectionnez l'onglet **Hôtes RDS**.

4 Sélectionnez un hôte RDS et cliquez sur **Plus de commandes**.

5 Cliquez sur **Activer** ou **Désactiver**.

6 Cliquez sur **OK**.

Si vous activez l'hôte RDS, une coche s'affiche dans la colonne Activé, et Disponible s'affiche dans la colonne État. Si vous désactivez l'hôte RDS, la colonne Activé est vide et Désactivé s'affiche dans la colonne État.

Surveiller les hôtes RDS

Vous pouvez surveiller l'état et afficher les propriétés des hôtes RDS dans View Administrator.

Procédure

◆ Dans View Administrator, accédez à la page qui affiche les propriétés que vous voulez consulter.

Propriétés	Action
Hôte RDS, Batterie de serveurs, Pool de postes de travail, Version d'agent, Sessions, État	■ Dans View Administrator, sélectionnez **Ressources > Machines**. ■ Cliquez sur l'onglet **Hôtes RDS**. Les hôtes RDS de clone lié et les hôtes RDS qui sont configurés manuellement sont affichés.
Nom DNS, Type, Batterie de serveurs RDS, Nombre max. de connexions, Version d'agent, Activé, État	■ Dans View Administrator, sélectionnez **Configuration de View > Machines inscrites**. ■ Cliquez sur l'onglet **Hôtes RDS**. Seuls les hôtes RDS qui sont configurés manuellement sont affichés.

Les propriétés s'affichent et ont les significations suivantes :

Propriété	Description
Hôte RDS	Nom de l'hôte RDS.
Batterie de serveurs	Batterie de serveurs à laquelle l'hôte RDS appartient.
Pool de postes de travail	Pool de postes de travail RDS associé à la batterie de serveurs.
Version d'agent	Version de View Agent ou d'Horizon Agent qui s'exécute sur l'hôte RDS.
Sessions	Nombre de sessions clientes.
Nom DNS	Nom DNS de l'hôte RDS.
Type	Version de Windows Server qui s'exécute sur l'hôte RDS.
Batterie de serveurs RDS	Batterie de serveurs à laquelle l'hôte RDS appartient.
Nombre max. de connexions	Nombre maximal de connexions que l'hôte RDS peut prendre en charge.
Activé	Indication précisant si l'hôte RDS est activé.
État	État de l'hôte RDS. Reportez-vous à « État des hôtes RDS », page 227 pour une description des états possibles.

État des hôtes RDS

Un hôte RDS peut être dans différents états après son initialisation. Nous vous recommandons de vérifier que les hôtes RDS sont dans l'état attendu avant et après l'exécution de tâches ou d'opérations les affectant.

Tableau 11-1. État d'un hôte RDS

État	Description
Démarrage	View Agent ou Horizon Agent a démarré sur l'hôte RDS mais d'autres services requis, comme le protocole d'affichage, sont toujours en cours de démarrage. La période de démarrage de l'agent permet également à d'autres processus, tels que les services de protocole, de démarrer.
Désactivation en cours	L'hôte RDS est en cours de désactivation, alors que les sessions continuent de s'exécuter sur l'hôte. Lorsque les sessions prennent fin, l'état passe à Désactivé.
Désactivé	Le processus de désactivation de l'hôte RDS est terminé.
Validation	Cet état se produit lorsque le Serveur de connexion View détecte l'hôte RDS pour la première fois, en général après le démarrage ou le redémarrage du Serveur de connexion View, et avant la première communication réussie avec View Agent ou Horizon Agent sur l'hôte RDS. Cet état est généralement temporaire. Cet état n'est pas le même que l'état Agent inaccessible, qui indique un problème de communication.
Agent désactivé	Se produit si le Serveur de connexion View désactive View Agent ou Horizon Agent. Il empêche le démarrage d'une nouvelle session de poste de travail ou d'application sur l'hôte RDS.
Agent inaccessible	Le Serveur de connexion View ne parvient pas à établir de communication avec View Agent ou Horizon Agent sur un hôte RDS.
IP non valide	Le paramètre de registre Masque de sous-réseau est configuré sur l'hôte RDS et aucun adaptateur réseau actif ne dispose d'une adresse IP dans la plage configurée.
L'agent doit redémarrer	Le composant de View a été mis à niveau et l'hôte RDS doit être redémarré pour permettre à View Agent ou Horizon Agent de fonctionner avec le composant mis à niveau.
Échec du protocole	Le protocole d'affichage RDP ne fonctionne pas correctement. Si RDP n'est pas en cours d'exécution, alors que PCoIP l'est, les clients ne peuvent pas se connecter via RDP ou PCoIP. En revanche, si RDP est en cours d'exécution, alors que PCoIP ne l'est pas, les clients peuvent se connecter via RDP.
Échec du domaine	L'hôte RDS a rencontré un problème en tentant d'atteindre le domaine. Le serveur de domaine n'était pas accessible ou l'authentification de domaine a échoué.
Erreur de configuration	Le rôle RDS n'est pas activé sur le serveur.
Inconnu	L'état de l'hôte RDS est inconnu.
Disponible	L'hôte RDS est disponible. Si l'hôte est situé dans une batterie de serveurs et si celle-ci est associée à un pool de RDS ou d'applications, il sera utilisé pour fournir des postes de travail et des applications RDS aux utilisateurs.
Approvisionnement	(Pour les hôtes RDS de clone lié uniquement) Le provisionnement de la machine virtuelle est en cours.
Personnalisation	(Pour les hôtes RDS de clone lié uniquement) La personnalisation de la machine virtuelle est en cours.
Suppression	(Pour les hôtes RDS de clone lié uniquement) La suppression de la machine virtuelle est en cours.
Attente d'agent	(Pour les hôtes RDS de clone lié uniquement) Le Serveur de connexion View attend pour établir la communication avec View Agent ou Horizon Agent.
Mode maintenance	(Pour les hôtes RDS de clone lié uniquement) La machine virtuelle est en mode de maintenance et n'est pas disponible pour les utilisateurs.
Approvisionné	(Pour les hôtes RDS de clone lié uniquement) Le provisionnement de la machine virtuelle est terminé.

Tableau 11-1. État d'un hôte RDS (suite)

État	Description
Erreur de provisionnement	(Pour les hôtes RDS de clone lié uniquement) Une erreur s'est produite lors du provisionnement.
Erreur	(Pour les hôtes RDS de clone lié uniquement) Une erreur inconnue s'est produite dans la machine virtuelle.

Configurer la limitation d'Adobe Flash avec Internet Explorer sur des postes de travail RDS

Pour s'assurer que la limitation d'Adobe Flash fonctionne avec Internet Explorer sur des postes de travail RDS, les utilisateurs doivent activer des extensions de navigateur tiers.

Procédure

1 Démarrez Horizon Client et connectez-vous au poste de travail distant d'un utilisateur.

2 Dans Internet Explorer, cliquez sur **Outils > Options Internet**.

3 Cliquez sur l'onglet **Avancé**, sélectionnez **Activer les extensions tierce partie du navigateur**, puis cliquez sur **OK**.

4 Redémarrez Internet Explorer.

Configuration de l'équilibrage de charge pour des hôtes RDS

Par défaut, le Serveur de connexion View utilise le nombre et la limite de session actuels pour équilibrer le placement de nouvelles sessions d'application sur les hôtes RDS. Vous pouvez remplacer ce comportement par défaut et contrôler le placement de nouvelles sessions d'application en écrivant et en configurant des scripts d'équilibrage de charge.

Un script d'équilibrage de charge renvoie une valeur de charge. La valeur de charge peut être basée sur n'importe quelle mesure d'hôte, telle que l'utilisation des CPU ou l'utilisation de la mémoire. Horizon Agent mappe la valeur de charge sur une préférence de charge et signale la préférence de charge au Serveur de connexion View. Le Serveur de connexion View utilise les préférences de charge signalées pour déterminer où placer les nouvelles sessions d'application.

Vous pouvez écrire vos propres scripts d'équilibrage de charge ou utiliser l'un des exemples de scripts d'équilibrage de charge fournis avec Horizon Agent.

La configuration de scripts d'équilibrage de charge implique d'activer le service VMware Horizon View Script Host et de définir une clé de registre sur chaque hôte RDS dans une batterie de serveurs.

Valeurs de charge et préférences de charge mappées

Horizon Agent mappe la valeur de charge qu'un script d'équilibrage de charge renvoie à une préférence de charge. Le Serveur de connexion View utilise les préférences de charge signalées pour déterminer où placer les nouvelles sessions d'application.

Le tableau suivant répertorie les valeurs de charge valides qu'un script d'équilibrage de charge peut renvoyer et décrit les préférences de charge associées.

Tableau 11-2. Valeurs de charge valides et préférences de charge mappées

Valeur de charge valide	Préférence de charge signalée par Horizon Agent	Description
0	BLOCK	Ne choisissez pas cet hôte RDS.
1	LOW	Préférence faible/charge élevée.
2	MED	Préférence moyenne/charge normale.
3	HIGH	Préférence élevée/charge légère.

Contraintes de la fonctionnalité d'équilibrage de charge

La fonctionnalité d'équilibrage de charge de l'hôte RDS présente certaines contraintes.

- Des règles anti-affinité peuvent empêcher une application d'être placée sur un hôte RDS, quelle que soit la préférence de charge signalée. Pour plus d'informations, reportez-vous à la section « Configurer une règle anti-affinité pour un pool d'applications », page 235.
- L'équilibrage de charge affecte uniquement les nouvelles sessions d'application. Un hôte RDS qui contient des sessions dans lesquelles un utilisateur a précédemment exécuté une application est toujours réutilisé pour la même application. Ce comportement remplace les préférences de charge signalées et les règles anti-affinité.
- Les applications sont lancées sur un hôte RDS où un utilisateur dispose déjà d'une session existante, même si l'hôte RDS signale une préférence de charge BLOCK.
- Les limites de session RDS empêchent la création de sessions d'application, quelle que soit la préférence de charge signalée.

Écrire un script d'équilibrage de charge pour un hôte RDS

Vous pouvez écrire un script d'équilibrage de charge pour générer une valeur de charge basée sur n'importe quelle mesure d'hôte RDS que vous voulez utiliser pour l'équilibrage de charge. Vous pouvez également écrire un script d'équilibrage de charge simple qui renvoie une valeur de charge fixe.

Votre script d'équilibrage de charge doit renvoyer un chiffre compris entre 0 et 3. Pour voir des descriptions des valeurs de charge valides, reportez-vous à la section « Valeurs de charge et préférences de charge mappées », page 228.

Si, dans la batterie de serveurs, au moins un hôte RDS renvoie une valeur de charge valide, le Serveur de connexion View suppose une valeur de charge de 2 (préférence de charge mappée MED) pour les autres hôtes RDS dans la batterie de serveurs jusqu'à ce que leurs scripts d'équilibrage de charge renvoient des valeurs valides. Si aucun hôte RDS dans la batterie de serveurs ne renvoie une valeur de charge valide, la fonctionnalité d'équilibrage de charge est désactivée pour la batterie de serveurs.

Si votre script d'équilibrage de charge renvoie une valeur de charge non valide ou si son exécution ne se termine pas dans les 10 secondes, Horizon Agent définit la préférence de charge sur BLOCK et l'état de l'hôte RDS sur une erreur de configuration. Ces valeurs suppriment effectivement l'hôte RDS de la liste d'hôtes RDS disponibles pour les nouvelles sessions.

Copiez votre script d'équilibrage de charge dans le répertoire `scripts` de Horizon Agent (`C:\Program Files\VMware\VMware View\Agent\scripts`) sur chaque hôte RDS dans la batterie de serveurs. Vous devez copier le même script sur chaque hôte RDS dans la batterie de serveurs.

Pour voir un exemple d'écriture d'un script d'équilibrage de charge, consultez les exemples de scripts dans le répertoire `scripts` d'Horizon Agent. Pour plus d'informations, reportez-vous à la section « Exemples de scripts d'équilibrage de charge pour des hôtes RDS », page 230.

Exemples de scripts d'équilibrage de charge pour des hôtes RDS

Lorsque vous installez Horizon Agent sur un hôte RDS, le programme d'installation place des exemples de scripts d'équilibrage de charge dans le répertoire `scripts` de Horizon Agent (`C:\Program Files\VMware\VMware View\Agent\scripts`).

Tableau 11-3. Exemples de scripts d'équilibrage de charge

Nom	Description
`cpuutilisation.vbs`	Lit le pourcentage de CPU qui a été utilisé dans le registre et renvoie les valeurs de charge suivantes : ■ 0, si l'utilisation de CPU est supérieure à 90 % ■ 1, si l'utilisation de CPU est supérieure à 75 % ■ 2, si l'utilisation de CPU est supérieure à 25 % ■ 3, si l'utilisation de CPU est inférieure ou égale à 25 %
`memoryutilisation.vbs`	Calcule le pourcentage de mémoire qui a été utilisé et renvoie les valeurs de charge suivantes : ■ 0, si l'utilisation de mémoire est supérieure à 90 % ■ 1, si l'utilisation de mémoire est supérieure à 75 % ■ 2, si l'utilisation de mémoire est supérieure à 25 % ■ 3, si l'utilisation de mémoire est inférieure ou égale à 25 %

Remarque Comme le script `cpuutilisation.vbs` utilise des données moyennes enchaînées échantillonnées toutes les cinq minutes, les événements hautement utilisés à court terme peuvent ne pas être reflétés dans les préférences de charge signalées. Vous pouvez réduire la période d'échantillonnage à un minimum de deux minutes, mais cela peut affecter les performances sur l'hôte RDS. L'intervalle d'échantillonnage est contrôlé par l'entrée de registre `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Performance Stats\SamplingIntervalSeconds`. La valeur par défaut est de 300 secondes.

Activer le service VMware Horizon View Script Host sur un hôte RDS

Vous devez activer le service VMware Horizon View Script Host sur un hôte RDS avant de configurer un script d'équilibrage de charge. Le service VMware Horizon View Script Host est désactivé par défaut.

Procédure

1 Connectez-vous à l'hôte RDS en tant qu'administrateur.

2 Démarrez le gestionnaire de serveurs.

3 Sélectionnez **Outils > Services** et accédez au service VMware Horizon View Script Host.

4 Cliquez avec le bouton droit sur **VMware Horizon View Script Host** et sélectionnez **Propriétés**.

5 Dans la boîte de dialogue Propriétés, sélectionnez **Automatique** dans le menu déroulant **Type de démarrage** et cliquez sur **OK** pour enregistrer vos modifications.

6 Cliquez avec le bouton droit sur **VMware Horizon View Script Host** et sélectionnez **Démarrer** pour démarrer le service VMware Horizon View Script Host.

Le service VMware Horizon View Script Host redémarre automatiquement chaque fois que l'hôte RDS démarre.

Suivant

Configurez votre script d'équilibrage de charge sur chaque hôte RDS dans la batterie de serveurs. Reportez-vous à la section « Configurer un script d'équilibrage de charge sur un hôte RDS », page 231.

Configurer un script d'équilibrage de charge sur un hôte RDS

Vous devez configurer le même script d'équilibrage de charge sur chaque hôte RDS dans la batterie de serveurs. La configuration d'un script d'équilibrage de charge implique la définition d'une clé de registre sur l'hôte RDS.

Si vous utilisez une batterie de serveurs automatisée, vous exécutez cette procédure sur la machine virtuelle parente pour la batterie de serveurs automatisée.

Important Vous devez configurer le script d'équilibrage de charge sur tous les hôtes RDS dans une batterie de serveurs ou sur aucun des hôtes RDS dans une batterie de serveurs. Si vous configurez un script d'équilibrage de charge uniquement sur certains hôtes RDS dans une batterie de serveurs, View Administrator définit la santé de la batterie de serveurs en jaune.

Prérequis

- Écrivez un script d'équilibrage de charge et copiez le même script dans le répertoire `scripts` d'Horizon Agent sur chaque hôte RDS dans la batterie de serveurs. Reportez-vous à la section « Écrire un script d'équilibrage de charge pour un hôte RDS », page 229.
- Activez le service VMware Horizon View Script Host sur l'hôte RDS. Reportez-vous à la section « Activer le service VMware Horizon View Script Host sur un hôte RDS », page 230.

Procédure

1. Connectez-vous à l'hôte RDS en tant qu'administrateur.
2. Démarrez le gestionnaire de serveurs.
3. Sélectionnez **Outils > Configuration système**, cliquez sur l'onglet **Outils** et lancez l'Éditeur de Registre.
4. Dans le registre, accédez à `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\ScriptEvents`.
5. Dans la zone de navigation, sélectionnez la touche **RdshLoad**.

   Les valeurs éventuelles de la touche **RdshLoad** s'affichent dans la zone de rubrique (volet de droite).
6. Cliquez avec le bouton droit sur la zone de rubrique de la touche **RdshLoad**, sélectionnez **Nouveau > Valeur de chaîne** et créez une nouvelle valeur de chaîne.

   Il vous est conseillé d'utiliser un nom qui représente le script d'équilibrage de charge à exécuter, par exemple, **`cpuutilisationScript`** pour le script `cpuutilisation.vbs`.
7. Cliquez avec le bouton droit sur l'entrée pour la nouvelle valeur de chaîne que vous avez créée et sélectionnez **Modifier**.
8. Dans le champ **Données de valeur**, saisissez la ligne de commande qui appelle votre script d'équilibrage de charge et cliquez sur **OK**.

   Saisissez le chemin complet vers votre script d'équilibrage de charge.

   Par exemple : `cscript.exe "C:\Program Files\VMware\VMware View Agent\scripts\cpuutilisation.vbs"`
9. Redémarrez le service Horizon Agent sur l'hôte RDS pour que les modifications prennent effet.

Votre script d'équilibrage de charge commence à s'exécuter sur l'hôte RDS.

Suivant

Répétez cette procédure sur chaque hôte RDS dans la batterie de serveurs. Si vous avez exécuté cette procédure sur la machine virtuelle parente pour une batterie de serveurs automatisée, provisionnez la batterie de serveurs automatisée.

Pour vérifier que votre script d'équilibrage de charge fonctionne correctement, reportez-vous à la section « Vérifier un script d'équilibrage de charge », page 232.

Vérifier un script d'équilibrage de charge

Vous pouvez vérifier que votre script d'équilibrage de charge fonctionne correctement en consultant les informations sur la batterie RDS et l'hôte RDS dans View Administrator.

Procédure

1 Dans View Administrator, cliquez sur **Tableau de bord** et développez **RDS Farms (Batteries RDS)** dans le volet Santé du système.

2 Consultez la santé de la batterie qui contient les hôtes RDS.

L'indicateur de santé de la batterie doit être vert. Si un script d'équilibrage de charge est configuré uniquement sur certains hôtes RDS dans une batterie de serveurs, View Administrator définit la santé de la batterie de serveurs sur jaune. Vous devez configurer le script d'équilibrage de charge sur tous les hôtes RDS dans une batterie de serveurs ou sur aucun des hôtes RDS dans une batterie de serveurs.

3 Développez la batterie et cliquez sur le nom de chaque hôte RDS pour consulter ses préférences de charge.

Le champ Charge du serveur de la boîte de dialogue des détails indique les préférences de charge rapportées par Horizon Agent, par exemple `Charge légère, nouvelles sessions OK`. Si Horizon Agent n'a pas signalé de préférence de charge, le champ Charge de serveur indique `Charge non signalée`.

Suivant

Si l'équilibrage de charge ne fonctionne pas comme prévu, vérifiez le contenu de votre script d'équilibrage de charge. Si le script est écrit correctement, vérifiez que le service VMware Horizon View Script Host est en cours d'exécution et que le même script d'équilibrage de charge est configuré sur chaque hôte RDS dans la batterie de serveurs.

Exemples de placement de session d'équilibrage de charge

Ces exemples illustrent deux scénarios de placement de session d'équilibrage de charge.

Exemple 1 : aucune session utilisateur existante

Cet exemple illustre comment le placement de session peut se produire pour une batterie de serveurs qui contient six hôtes RDS lorsqu'il n'existe actuellement aucune session utilisateur sur l'un des hôtes RDS.

1 Horizon Agent signale les préférences de charge suivantes pour chaque hôte RDS dans la batterie de serveurs.

Hôte RDS	Préférence de charge
1	HIGH
2	LOW
3	HIGH
4	MED
5	BLOCK
6	LOW

2 View trie les hôtes RDS en trois compartiments en fonction de la préférence de charge. View ignore l'hôte RDS 5, car Horizon Agent a signalé la préférence de charge BLOCK.

Compartiment	Préférence de charge	Hôte RDS
1	HIGH	1
	HIGH	3
2	MED	4
3	LOW	2
	LOW	6

3 Comme le compartiment 2 ne contient qu'un seul hôte RDS, View combine le compartiment 2 et le compartiment 3

Compartiment	Préférence de charge	Hôte RDS
1	HIGH	1
	HIGH	3
	MED	4
2	LOW	2
	LOW	6

4 View classe les compartiments de façon aléatoire.

Compartiment	Préférence de charge	Hôte RDS
1	MED	4
	HIGH	3
	MED	1
2	LOW	6
	LOW	2

5 Le Serveur de connexion View tente de placer une nouvelle session d'application sur l'hôte RDS 4 en premier, puis sur l'hôte RDS 3, etc.

Ordre de placement de session d'hôte RDS
4
3
1
6
2

Remarque Des règles anti-affinité peuvent empêcher une application d'être placée sur un hôte RDS, quelle que soit la préférence de charge signalée. Pour plus d'informations, reportez-vous à la section « Configurer une règle anti-affinité pour un pool d'applications », page 235.

Exemple 2 : session utilisateur existante

Cet exemple illustre comment le placement de session peut se produire pour une batterie de serveurs qui contient six hôtes RDS lorsqu'une session utilisateur existe actuellement sur l'un des hôtes RDS. Un hôte RDS qui contient une session dans laquelle un utilisateur a précédemment exécuté une application est toujours réutilisé pour la même application.

1 Une session utilisateur existe déjà sur l'hôte RDS 3. L'hôte RDS 3 a la préférence de charge MED. Les hôtes RDS restants dans la batterie de serveurs (la liste de rechange) ont les préférences de charge suivantes.

Hôte RDS	Préférence de charge
1	MED
2	LOW
4	HIGH
5	LOW
6	BLOCK

2 View trie les hôtes RDS dans la liste de rechange en deux compartiments en fonction de la préférence de charge. View ignore l'hôte RDS 6, car Horizon Agent a signalé la préférence de charge BLOCK.

Compartiment	Préférence de charge	Hôte RDS
1	HIGH	4
	MED	1
2	LOW	2
	LOW	5

3 View classe les compartiments de façon aléatoire.

Compartiment	Préférence de charge	Hôte RDS
1	HIGH	4
	MED	1
2	LOW	5
	LOW	2

4 View ajoute l'hôte RDS qui contient la session existante au début de la liste classée de compartiments.

Ordre de placement de session d'hôte RDS
3
4
1
5
2

Configurer une règle anti-affinité pour un pool d'applications

Lorsque vous configurez une règle anti-affinité pour un pool d'applications, le Serveur de connexion Horizon tente de lancer l'application uniquement sur des hôtes RDS disposant de suffisamment de ressources pour exécuter l'application. Cette fonctionnalité peut être utile pour contrôler des applications qui consomment de grandes quantités de CPU ou de ressources de mémoire.

Une règle anti-affinité se compose d'un modèle de correspondance d'application et d'un nombre maximal. Par exemple, le modèle de correspondance d'application peut être `autocad.exe` et le nombre maximal 2.

Le Serveur de connexion envoie la règle anti-affinité à Horizon Agent sur un hôte RDS. Si des applications exécutées sur l'hôte RDS possèdent des noms de processus qui correspondent au modèle de correspondance d'application, Horizon Agent compte le nombre actuel d'instances de ces applications et le compare au nombre maximal. Si le nombre maximal est dépassé, le Serveur de connexion ignore cet hôte RDS lorsqu'il sélectionne un hôte RDS pour exécuter de nouvelles sessions de l'application.

Prérequis

- Créez le pool d'applications. Consultez la section « Création de pools d'applications » du document *Configuration d'applications et de postes de travail publiés dans Horizon 7*.
- Familiarisez-vous avec les contraintes de la fonctionnalité anti-affinité. Reportez-vous à la section « Contraintes de la fonctionnalité anti-affinité », page 235.

Procédure

1. Dans Horizon Administrator, sélectionnez **Catalogue > Pools d'applications**.
2. Sélectionnez le pool à modifier et cliquez sur **Modifier**.
3. Dans la zone de texte **Modèles d'anti-affinité**, saisissez une liste séparée par des virgules de modèles à comparer aux noms de processus d'autres applications exécutées sur des hôtes RDS.

   La chaîne de modèle peut inclure les caractères génériques astérisque (*) et point d'interrogation (?) . L'astérisque correspond à zéro caractère ou plus et le point d'interrogation correspond à un seul caractère.

   Par exemple, **`*pad.exe,*notepad.???`** correspond à `wordpad.exe`, `notepad.exe` et `notepad.bat`, mais il ne correspond pas à `wordpad.bat` ni à `notepad.script`.

   Remarque Horizon 7 compte plusieurs modèles qui correspondent à une application dans une session comme une seule correspondance.

4. Dans la zone de texte **Nombre d'anti-affinités**, saisissez le nombre maximal d'autres applications pouvant être exécutées sur l'hôte RDS avant que l'hôte RDS soit refusé pour les nouvelles sessions d'application.

   Le nombre maximal peut être un entier allant de 1 à 20.

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

Contraintes de la fonctionnalité anti-affinité

La fonctionnalité anti-affinité a certaines contraintes.

- Les règles anti-affinité affectent uniquement les nouvelles sessions d'application. Un hôte RDS qui contient des sessions dans lesquelles un utilisateur a précédemment exécuté une application est toujours réutilisé pour la même application. Ce comportement remplace les préférences de charge signalées et les règles anti-affinité.
- Les règles anti-affinité n'affectent pas les lancements d'application dans une session de poste de travail RDS.

- Les limites de session RDS empêchent la création de sessions d'application, quelles que soient les règles anti-affinité.
- Dans certaines circonstances, les instances d’applications sur l’hôte RDS peuvent ne pas être limitées au nombre maximal que vous spécifiez. Par exemple, View ne peut pas déterminer le nombre exact d'instances si d'autres applications pour d'autres sessions en attente sont en cours de lancement.
- Les règles anti-affinité entre applications ne sont pas prises en charge. Par exemple, les classes d'application importantes, telles que les instances Autocad et Visual Studio, ne peuvent pas être comptées dans une seule règle.
- N'utilisez pas de règles anti-affinité dans des environnements où les utilisateurs finaux utilisent Horizon Client sur des clients mobiles. Les règles anti-affinité peuvent être à l'origine de plusieurs sessions dans la même batterie pour un utilisateur final. La reconnexion à plusieurs sessions sur des clients mobiles peut entraîner un comportement indéterminé.

Gestion d'applications ThinApp dans View Administrator 12

Vous pouvez utiliser View Administrator pour distribuer et gérer des applications modularisées avec VMware ThinApp. La gestion d'applications ThinApp dans View Administrator implique la capture et le stockage de modules d'applications, l'ajout d'applications ThinApp à View Administrator et l'attribution d'applications ThinApp à des machines et des pools de postes de travail.

Vous devez posséder une licence pour utiliser la fonction de gestion ThinApp dans View Administrator.

Important Si, plutôt que distribuer des applications ThinApp en les attribuant à des machines et des pools de postes de travail, vous préférez attribuer des applications ThinApp à des utilisateurs et à des groupes Active Directory, vous pouvez utiliser VMware Identity Manager.

Ce chapitre aborde les rubriques suivantes :

Configuration requise de View pour des applications ThinApp

Lorsque vous capturez et stockez des applications ThinApp qui seront distribuées sur des postes de travail distants dans View Administrator, vous devez respecter un certain nombre d'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 réseau Windows qui réside dans un domaine Active Directory et qui est accessible par votre hôte du Serveur de connexion View et par vos postes de travail distants. 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 modules d'applications ThinApp diffusés en continu, vous devez définir l'autorisation NTFS du partage réseau qui héberge les modules ThinApp sur `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 diffusées en continu sur des postes de travail distants, les utilisateurs doivent disposer d'un accès au partage 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 239

Vous utilisez l'assistant ThinApp Setup Capture pour capturer et assembler vos applications.

2 Créer un partage de réseau Windows page 239

Vous devez créer un partage réseau Windows pour héberger les packages MSI distribués aux postes de travail et aux pools distants dans View Administrator.

3 Enregistrer un référentiel d'applications page 240

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 240

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'attribuer à des machines et à des pools de postes de travail.

5 Créer un modèle d'application ThinApp page 241

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/products/thinapp et installez-le sur un ordinateur sain. View prend en charge ThinApp version 4.6 et supérieure.
- Familiarisez-vous avec la configuration logicielle requise pour ThinApp et les instructions d'assemblage des applications dans le *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 **Créer un package MSI**.

3 Si vous prévoyez de diffuser en continu l'application sur des postes de travail distants, 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 réseau Windows pour héberger les packages MSI distribués aux postes de travail et aux pools distants dans View Administrator.

Prérequis

- Utilisez l'assistant ThinApp Capture Setup pour assembler les applications.
- Vérifiez que le partage réseau répond aux exigences de View en matière de stockage d'applications ThinApp. Pour plus d'informations, reportez-vous à « Configuration requise de View pour des applications ThinApp », page 237.

Procédure

1 Créez un dossier partagé sur un ordinateur dans un domaine Active Directory accessible à votre hôte du Serveur de connexion View et à vos postes de travail distants.

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 modules d'applications ThinApp diffusés en continu, définissez l'autorisation NTFS du partage réseau qui héberge les modules ThinApp sur `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 **Configuration de View > Configuration d'application ThinApp** et cliquez sur **Ajouter un référentiel**.

2 Saisissez un nom d'affichage pour le référentiel d'applications dans la zone de texte **Nom d'affichage**.

3 Saisissez le chemin vers le partage de réseau Windows qui héberge vos packages d'applications dans la zone de texte **Partager un chemin d'accès**.

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 **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'attribuer à des machines et à des pools de postes de travail.

Prérequis

Enregistrez un référentiel d'applications avec View Administrator.

Procédure

1 Dans View Administrator, sélectionnez **Catalogue > ThinApps**.

2 Sous l'onglet **Résumé**, cliquez sur **Analyser de nouvelles ThinApps**.

3 Sélectionnez un référentiel d'applications et un dossier à analyser et cliquez sur **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 **Analyser** pour commencer à analyser les packages MSI que vous avez sélectionnés.

Vous pouvez cliquer sur **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 **Terminer**.

Les nouvelles applications ThinApp apparaissent sous l'onglet **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 attribuez un modèle ThinApp à un pool de machines ou de postes de travail, 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 ThinApp après avoir attribué celui-ci à un pool de machines ou de postes de travail, View Administrator n'attribue pas automatiquement la nouvelle application au pool de machines ou de postes de travail. Si vous supprimez une application d'un modèle ThinApp qui était précédemment attribué à un pool de machines ou de postes de travail, l'application reste attribuée au pool de machines ou de postes de travail.

Prérequis

Ajoutez des applications ThinApp sélectionnées à View Administrator.

Procédure

1 Dans View Administrator, sélectionnez **Catalogue > ThinApps** et cliquez sur **Nouveau modèle**.

2 Saisissez un nom pour le modèle et cliquez sur **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 **Rechercher** et cliquez sur **Rechercher**.

4 Sélectionnez les applications ThinApp que vous voulez inclure dans le modèle et cliquez sur **Ajouter**.

Vous pouvez appuyer sur Ctrl+clic ou Maj+clic pour sélectionner plusieurs applications.

5 Cliquez sur **OK** pour enregistrer le modèle.

Attribution d'applications ThinApp à des machines et à des pools de postes de travail

Pour installer une application ThinApp sur un poste de travail distant, vous pouvez utiliser View Administrator pour attribuer l'application ThinApp à une machine ou à un pool de postes de travail.

Lorsque vous attribuez une application ThinApp à une machine, View Administrator commence l'installation de l'application sur la machine virtuelle quelques minutes plus tard. Lorsque vous attribuez une application ThinApp à un pool de postes de travail, View Administrator commence l'installation de l'application la première fois qu'un utilisateur se connecte à un poste de travail distant du pool.

Diffusion en continu	View Administrator installe un raccourci vers l'application ThinApp sur le poste de travail distant. 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.
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 attribuer des applications ThinApp à des postes de travail basés sur une machine virtuelle et à des pools de postes de travail automatisés ou manuels qui contiennent des machines virtuelles vCenter Server. Vous ne pouvez pas attribuer des applications ThinApp à des postes de travail RDS ou à des PC traditionnels.

Meilleures pratiques pour l'affectation d'applications ThinApp

Respectez les recommandations lorsque vous attribuez des applications ThinApp à des machines et à des pools de postes de travail.

- Pour installer une application ThinApp sur un poste de travail distant particulier, attribuez l'application à la machine virtuelle qui héberge le poste de travail. Si vous utilisez une convention de dénomination commune pour vos machines, vous pouvez utiliser les attributions de machine pour distribuer rapidement les applications à toutes les machines utilisant une convention de dénomination commune.
- Pour installer une application ThinApp sur toutes les machines d'un pool de postes de travail, attribuez l'application au pool de postes de travail. Si vous organisez vos pools de poste de travail par type de service ou d'utilisateur, vous pouvez utiliser des attributions de pool de postes de travail pour distribuer rapidement les applications à des services ou à des utilisateurs spécifiques. Par exemple, si vous disposez d'un pool de postes de travail pour les utilisateurs du service de comptabilité, vous pouvez distribuer la même application à l'ensemble des utilisateurs du service en attribuant l'application au pool de comptabilité.
- Pour rationaliser la distribution de plusieurs applications ThinApp, incluez les applications dans un modèle d'application ThinApp. Lorsque vous attribuez un modèle ThinApp à une machine ou à un pool de postes de travail, View Administrator installe l'ensemble des applications se trouvant actuellement dans le modèle.
- N'attribuez pas de modèle ThinApp à une machine ou à un pool de postes de travail si le modèle contient une application ThinApp déjà attribuée à cette machine ou à ce pool de postes de travail. N'attribuez pas non plus à plusieurs reprises un modèle ThinApp à une même machine ou à un même pool de postes de travail avec un autre type d'installation. View Administrator renverra des erreurs d'affectation ThinApp dans ces deux situations.

Attribuer une application ThinApp à plusieurs machines

Vous pouvez attribuer une application ThinApp particulière à une ou plusieurs machines.

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 240.

Procédure

1 Dans View Administrator, sélectionnez **Catalogue > ThinApps** et sélectionnez l'application ThinApp.

2 Sélectionnez **Affecter des machines** dans le menu déroulant **Ajouter une affectation**.

Les machines auxquelles l'application ThinApp n'est pas déjà attribuée s'affichent dans le tableau.

Option	Action
Rechercher une machine spécifique	Tapez le nom de la machine dans la zone de texte **Rechercher**, puis cliquez sur **Rechercher**.
Rechercher toutes les machines qui suivent la même convention de dénomination	Tapez un nom de machine partiel dans la zone de texte **Rechercher**, puis cliquez sur **Rechercher**.

3 Sélectionnez les machines auxquelles vous souhaitez attribuer l'application ThinApp et cliquez sur **Ajouter**.

Vous pouvez appuyer sur Ctrl+clic ou Maj+clic pour sélectionner plusieurs machines.

4 Sélectionnez un type d'installation et cliquez sur **OK**.

Option	Action
Diffusion en continu	Installe un raccourci vers l'application sur la machine. 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.
Complète	Installe l'application complète sur le système de fichiers local de la machine.

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. Une fois l'installation terminée, l'application est disponible pour tous les utilisateurs des postes de travail distants hébergés par les machines virtuelles.

Attribuer plusieurs applications ThinApp à une machine

Vous pouvez attribuer une ou plusieurs applications ThinApp à une machine particulière.

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 240.

Procédure

1 Dans View Administrator, sélectionnez **Ressources > Machines** et double-cliquez sur le nom de la machine dans la colonne Machine.

2 Sous l'onglet **Résumé**, cliquez sur **Ajouter une affectation** dans le volet ThinApps.

Les applications ThinApp qui ne sont pas déjà attribuées à la machine s'affichent dans le tableau.

3 Pour rechercher une application particulière, saisissez le nom de l'application dans la zone de texte **Rechercher** et cliquez sur **Rechercher**.

4 Sélectionnez une application ThinApp à attribuer à la machine et cliquez sur **Ajouter**.

Répétez cette étape pour ajouter plusieurs applications.

5 Sélectionnez un type d'installation et cliquez sur **OK**.

Option	Action
Diffusion en continu	Installe un raccourci vers l'application sur la machine. 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.
Complète	Installe l'application complète sur le système de fichiers local de la machine.

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 distant hébergé par la machine virtuelle.

Attribuer une application ThinApp à plusieurs pools de postes de travail

Vous pouvez attribuer une application ThinApp particulière à un ou plusieurs pools de postes de travail.

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 240.

Procédure

1 Dans View Administrator, sélectionnez **Catalogue > ThinApps** et sélectionnez l'application ThinApp.

2 Sélectionnez **Attribuer des pools de postes de travail** dans le menu déroulant **Ajouter une affectation**.

Les pools de postes de travail auxquels l'application ThinApp n'est pas déjà attribuée figurent dans le tableau.

Option	Action
Rechercher un pool de postes de travail spécifique	Tapez le nom du pool de postes de travail dans la zone de texte **Rechercher**, puis cliquez sur **Rechercher**.
Rechercher tous les pools de postes de travail qui répondent à la même convention de dénomination	Tapez un nom partiel de pool de postes de travail dans la zone de texte **Rechercher**, puis cliquez sur **Rechercher**.

3 Sélectionnez les pools de postes de travail auxquels vous souhaitez attribuer l'application ThinApp, puis cliquez sur **Ajouter**.

Vous pouvez appuyer sur Ctrl+clic ou sur Maj+clic pour sélectionner plusieurs pools de postes de travail.

4 Sélectionnez un type d'installation et cliquez sur **OK**.

Option	Action
Diffusion en continu	Installe un raccourci vers l'application sur la machine. 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.
Complète	Installe l'application complète sur le système de fichiers local de la machine.

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. Une fois l'installation terminée, l'application est disponible pour tous les utilisateurs du pool de postes de travail.

Attribuer plusieurs applications ThinApp à un pool de postes de travail

Vous pouvez attribuer une ou plusieurs applications ThinApp à un pool de postes de travail 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 240.

Procédure

1 Dans View Administrator, sélectionnez **Catalogue > Pools de postes de travail** et double-cliquez sur l'ID du pool.

2 Sous l'onglet **Inventaire**, cliquez sur **ThinApps** et cliquez sur **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 **Rechercher** et cliquez sur **Rechercher**.

4 Sélectionnez une application ThinApp à affecter au pool et cliquez sur **Ajouter**.

Répétez cette étape pour sélectionner plusieurs applications.

5 Sélectionnez un type d'installation et cliquez sur **OK**.

Option	Action
Diffusion en continu	Installe un raccourci vers l'application sur la machine. 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.
Complète	Installe l'application complète sur le système de fichiers local de la machine.

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. Une fois l'installation terminée, les applications sont disponibles pour tous les utilisateurs du pool de postes de travail.

Attribuer un modèle ThinApp à une machine ou à un pool de postes de travail

Vous pouvez rationaliser la distribution de plusieurs applications ThinApp en attribuant un modèle ThinApp à une machine ou à un pool de postes de travail.

Lorsque vous attribuez un modèle ThinApp à une machine ou à un pool de postes de travail, View Administrator installe les applications ThinApp actuellement incluses dans le modèle.

Prérequis

Créez un modèle d'application ThinApp. Reportez-vous à

« Créer un modèle d'application ThinApp », page 241.

Procédure

1 Dans View Administrator, sélectionnez **Catalogue > ThinApps**.

2 Sélectionnez le modèle d'application ThinApp.

3 Sélectionnez **Attribuer des machines** ou **Attribuer des pools de postes de travail** dans le menu déroulant **Ajouter une affectation**.

Toutes les machines ou tous les pools de poste de travail s'affichent dans le tableau.

Option	Action
Trouver une machine ou un pool de postes de travail spécifique	Tapez le nom de la machine ou du pool de postes de travail dans la zone de texte **Rechercher** et cliquez sur **Rechercher**.
Rechercher toutes les machines et tous les pools de postes de travail qui répondent à la même convention de dénomination	Tapez un nom partiel de machine ou de pool de postes de travail dans la zone de texte **Rechercher** et cliquez sur **Rechercher**.

4 Sélectionnez les machines ou les pools de postes de travail auxquels vous souhaitez attribuer le modèle ThinApp et cliquez sur **Ajouter**.

Répétez cette étape pour sélectionner plusieurs machines ou plusieurs pools de postes de travail.

5 Sélectionnez un type d'installation et cliquez sur **OK**.

Option	Action
Diffusion en continu	Installe un raccourci vers l'application sur la machine. 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.
Complète	Installe l'application complète sur le système de fichiers local de la machine.

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 attribuez un modèle ThinApp à une machine, View Administrator commence l'installation des applications incluses dans le modèle quelque minutes plus tard. Lorsque vous attribuez un modèle ThinApp à un pool de postes de travail, View Administrator commence l'installation des applications incluses dans le modèle la première fois qu'un utilisateur se connecte à un poste de travail distant du pool de postes de travail. Une fois l'installation terminée, les applications sont disponibles pour tous les utilisateurs de la machine ou du pool de postes de travail.

View Administrator renvoie une erreur d'attribution d'application si un modèle ThinApp contient une application qui est déjà attribuée à la machine ou au pool de postes de travail.

Consulter des affectations d'application ThinApp

Vous pouvez vérifier l'ensemble des machines et des pools de postes de travail auxquels une application ThinApp particulière est actuellement attribuée. Vous pouvez également vérifier toutes les applications ThinApp attribuées à une machine ou à un pool de postes de travail particulier.

Prérequis

Familiarisez-vous avec les valeurs d'état d'installation de ThinApp dans la section « Valeurs d'état d'installation d'application ThinApp », page 248

Procédure

- Sélectionnez les affectations d'application ThinApp que vous voulez consulter.

Option	Action
Vérifier l'ensemble des machines et des pools de postes de travail auxquels une application ThinApp particulière est attribuée	Sélectionnez **Catalogue > ThinApps**, puis double-cliquez sur le nom de l'application ThinApp. L'onglet **Affectations** affiche les machines et les pools de postes de travail auxquels l'application est actuellement attribuée, ainsi que le type d'installation. L'onglet **Machines** affiche les machines qui sont actuellement associées à l'application, ainsi que les informations d'état de l'installation. **Remarque** Lorsque vous attribuez une application ThinApp à un pool, les machines du pool s'affichent sous l'onglet **Machines** uniquement après l'installation de l'application.
Vérifier toutes les applications ThinApp qui sont attribuées à une machine particulière	Sélectionnez **Ressources > Machines** et double-cliquez sur le nom de la machine dans la colonne Machine. Le volet ThinApps de l'onglet **Résumé** affiche chaque application qui est actuellement attribuée à la machine, ainsi que l'état de l'installation.
Vérifier toutes les applications ThinApp qui sont attribués à un pool de postes de travail particulier	Sélectionnez **Catalogue > Pools de postes de travail**, double-cliquez sur l'ID du pool, sélectionnez l'onglet **Inventaire**, puis cliquez sur **ThinApps**. Le volet Attributions ThinApp affiche chaque application qui est actuellement attribuée au pool de postes de travail.

Valeurs d'état d'installation d'application ThinApp

Après l'attribution d'une application ThinApp à une machine ou à un pool, View Administrator indique l'état de l'installation.

Tableau 12-1 décrit chaque valeur d'état.

Tableau 12-1. État de l'installation d'une application ThinApp

État	Description
Affecté	L'application ThinApp est attribuée à la machine.
Erreur d'installation	Une erreur s'est produite lorsque View Administrator a tenté d'installer l'application ThinApp.
Erreur de désinstallation	Une erreur s'est produite lorsque View Administrator a tenté de désinstaller l'application ThinApp.
Installé	L'application ThinApp est installée.
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 machines dans des pools de postes de travail.
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 **Catalogue > ThinApps**.

L'onglet **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 **Résumé** pour voir des informations générales sur le package MSI.

4 Cliquez sur **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 attribution d'application ThinApp à plusieurs machines page 249

  Vous pouvez supprimer l'attribution d'une application ThinApp particulière à une ou plusieurs machines.

- Supprimer l'attribution de plusieurs applications ThinApp à une machine page 250

  Vous pouvez supprimer l'attribution d'une ou de plusieurs applications ThinApp à une machine particulière.

- Supprimer une attribution d'application ThinApp de plusieurs pools de postes de travail page 250

  Vous pouvez supprimer d'un ou de plusieurs pools de postes de travail l'attribution d'une application ThinApp donnée.

- Supprimer plusieurs attributions d'applications ThinApp d'un pool de postes de travail page 251

  Vous pouvez supprimer une ou plusieurs attributions d'applications ThinApp d'un pool de postes de travail particulier.

- Supprimer une application ThinApp de View Administrator page 251

  Lorsque vous supprimez une application ThinApp de View Administrator, vous ne pouvez plus l'attribuer à des pools de machines et de postes de travail.

- Modifier ou supprimer un modèle d'application ThinApp page 251

  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 252

  Vous pouvez supprimer un référentiel d'applications de View Administrator.

Supprimer une attribution d'application ThinApp à plusieurs machines

Vous pouvez supprimer l'attribution d'une application ThinApp particulière à une ou plusieurs machines.

Prérequis

Informez les utilisateurs des postes de travail distants hébergés par les machines que vous prévoyez de supprimer l'application.

Procédure

1 Dans View Administrator, sélectionnez **Catalogue > ThinApps** et double-cliquez sur le nom de l'application ThinApp.

2 Dans l'onglet **Affectations**, sélectionnez une machine et cliquez sur **Supprimer une affectation**.

Vous pouvez appuyer sur Ctrl+clic ou Maj+clic pour sélectionner plusieurs machines.

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, commencez par désinstaller manuellement les fichiers de l'application ThinApp de la machine, puis cliquez sur **Supprimer l'état d'application du poste de travail** dans View Administrator.

Supprimer l'attribution de plusieurs applications ThinApp à une machine

Vous pouvez supprimer l'attribution d'une ou de plusieurs applications ThinApp à une machine particulière.

Prérequis

Informez les utilisateurs du poste de travail distant qui est hébergé par la machine que vous prévoyez de supprimer les applications.

Procédure

1 Dans View Administrator, sélectionnez **Ressources > Machines** et double-cliquez sur le nom de la machine dans la colonne Machine.

2 Sous l'onglet **Résumé**, sélectionnez l'application ThinApp et cliquez sur **Supprimer une affectation** dans le volet ThinApps.

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, commencez par désinstaller manuellement les fichiers de l'application ThinApp de la machine, puis cliquez sur **Supprimer l'état d'application du poste de travail** dans View Administrator.

Supprimer une attribution d'application ThinApp de plusieurs pools de postes de travail

Vous pouvez supprimer d'un ou de plusieurs pools de postes de travail l'attribution d'une application ThinApp donnée.

Prérequis

Informez les utilisateurs des postes de travail distants des pools que vous prévoyez de supprimer l'application.

Procédure

1 Dans View Administrator, sélectionnez **Catalogue > ThinApps** et double-cliquez sur le nom de l'application ThinApp.

2 Dans l'onglet **Affectations**, sélectionnez un pool de postes de travail et cliquez sur **Supprimer une affectation**.

Vous pouvez appuyer sur Ctrl+clic ou sur Maj+clic pour sélectionner plusieurs pools de postes de travail.

View Administrator désinstalle l'application ThinApp la première fois qu'un utilisateur ouvre une session sur un poste de travail distant du pool.

Supprimer plusieurs attributions d'applications ThinApp d'un pool de postes de travail

Vous pouvez supprimer une ou plusieurs attributions d'applications ThinApp d'un pool de postes de travail particulier.

Prérequis

Informez les utilisateurs des postes de travail distants du pool que vous prévoyez de supprimer les applications.

Procédure

1 Dans View Administrator, sélectionnez **Catalogue > Pools de postes de travail** et double-cliquez sur l'ID du pool.

2 Sous l'onglet **Inventaire**, cliquez sur **ThinApps**, sélectionnez l'application ThinApp et cliquez sur **Supprimer une affectation**.

Répétez cette étape pour supprimer plusieurs applications.

View Administrator désinstalle les applications ThinApp la première fois qu'un utilisateur se connecte sur un poste de travail distant du pool.

Supprimer une application ThinApp de View Administrator

Lorsque vous supprimez une application ThinApp de View Administrator, vous ne pouvez plus l'attribuer à des pools de machines et de postes de travail.

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 attribuée à un pool de machines ou de postes de travail, ou si elle se trouve dans l'état Désinstallation en attente.

Prérequis

Si une application ThinApp est actuellement attribuée à un pool de machines ou de postes de travail, supprimez l'attribution au pool de machines ou de postes de travail.

Procédure

1 Dans View Administrator, sélectionnez **Catalogue > ThinApps** et sélectionnez l'application ThinApp.

2 Cliquez sur **Supprimer une 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 ThinApp après avoir attribué celui-ci à un pool de machines ou de postes de travail, View Administrator n'attribue pas automatiquement la nouvelle application au pool de machines ou de postes de travail. Si vous supprimez une application d'un modèle ThinApp qui était précédemment attribué à un pool de machines ou de postes de travail, l'application reste attribuée au pool de machines ou de postes de travail.

Procédure

- Dans View Administrator, sélectionnez **Catalogue > ThinApps** et sélectionnez le modèle ThinApp.

Option	Action
Add or remove ThinApp applications from the template (Ajouter ou supprimer des applications ThinApp du modèle)	Cliquez sur **Modifier le modèle**.
Delete the template (Supprimer le modèle)	Cliquez sur **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 **Configuration de View > Configuration d'application ThinApp** et sélectionnez le référentiel d'applications.
2. Cliquez sur **Supprimer un 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 afficher ces événements sur la page **Événements** de View Administrator.

Un événement s'affiche sur la page **Événements** dans les cas suivants.

- Une application ThinApp est affectée ou une affectation d'application est supprimée.
- Une application ThinApp est installée ou désinstallée d'une machine
- 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 du Serveur de connexion View ne peut pas accéder au partage de réseau qui héberge le référentiel d'applications. Le chemin de partage de réseau que vous avez saisi dans la zone de texte **Partager un chemin d'accès** 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 du Serveur de connexion View 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 du Serveur de connexion View.
- 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 **Analyser de nouvelles ThinApps** dans View Administrator.

Cause

Les packages d'applications ne sont pas au format MSI ou l'hôte du Serveur de connexion View 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 237 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 252 pour plus d'informations.

Des messages apparaissent dans le fichier journal de débogage du Serveur de connexion View lorsqu'un référentiel d'applications est analysé. Les fichiers journaux du Serveur de connexion View sont situés sur l'hôte du Serveur de connexion View 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 attribuer un modèle d'application ThinApp à une machine ou à un pool de postes de travail.

Problème

View Administrator renvoie une erreur d'attribution lorsque vous tentez d'attribuer un modèle d'application ThinApp à une machine ou à un pool de postes de travail.

Cause

Le modèle d'application ThinApp contient une application qui est déjà attribuée à la machine ou au pool de postes de travail, ou le modèle d'application ThinApp était déjà affecté à la machine ou au pool de postes de travail avec un type d'installation différent.

Solution

Si le modèle contient une application ThinApp qui est déjà attribuée à la machine ou au pool de postes de travail, créez un modèle qui ne contient pas l'application ou modifiez le modèle existant et supprimez l'application. Attribuez le nouveau modèle ou le modèle modifié à la machine ou au pool de postes de travail.

Pour modifier le type d'installation d'une application ThinApp, vous devez supprimer l'attribution d'application existante de la machine ou du pool de postes de travail. Une fois l'application ThinApp désinstallée, vous pouvez l'attribuer à la machine ou au pool de postes de travail avec un autre type d'installation.

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 la machine était insuffisant pour installer l'application ThinApp.
- La connectivité réseau a été perdue entre l'hôte du Serveur de connexion View et la machine ou entre l'hôte du Serveur de connexion View 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 la machine.

Pour plus d'informations sur la cause du problème, vous pouvez consulter les fichiers journaux d'Horizon Agent et du Serveur de connexion View.

Les fichiers journaux d'Horizon Agent se trouvent sur la machine dans le répertoire *`lecteur`*`:\ProgramData\VMware\VDM\logs`.

Les fichiers journaux du Serveur de connexion View se trouvent sur l'hôte du Serveur de connexion View dans le répertoire *`drive`*`:\Documents and Settings\All Users\Application Data\VMware\VDM\logs`.

Solution

1 Dans View Administrator, sélectionnez **Catalogue > ThinApps**.

2 Cliquez sur le nom de l'application ThinApp.

3 Dans l'onglet **Machines**, sélectionnez la machine et cliquez sur **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 du Serveur de connexion View et la machine.

Pour plus d'informations sur la cause du problème, vous pouvez consulter les fichiers journaux d'Horizon Agent et du Serveur de connexion View.

Les fichiers journaux d'Horizon Agent sont situés sur la machine dans le répertoire *`lecteur`*`:\Documents and Settings\All Users\Application Data\VMware\VDM\logs` pour les systèmes Windows XP et dans le répertoire *`lecteur`*`:\ProgramData\VMware\VDM\logs` pour les systèmes Windows 7.

Les fichiers journaux du Serveur de connexion View se trouvent sur l'hôte du Serveur de connexion View dans le répertoire *`drive`*`:\Documents and Settings\All Users\Application Data\VMware\VDM\logs`.

Solution

1 Dans View Administrator, sélectionnez **Catalogue > ThinApps**.

2 Cliquez sur le nom de l'application ThinApp.

3 Cliquez sur l'onglet **Machines**, sélectionnez la machine et cliquez sur **Réessayer la désinstallation** pour recommencer l'opération de désinstallation.

4 Si l'opération de désinstallation échoue toujours, supprimez manuellement l'application ThinApp de la machine, puis cliquez sur **Supprimer l'état d'application du poste de travail**.

   Cette commande efface l'affectation d'application ThinApp dans View Administrator. Elle ne supprime aucun fichier ni aucun paramètre de la machine.

   Important N'utilisez cette commande qu'après avoir supprimé manuellement l'application ThinApp de la machine.

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 238
- « Attribution d'applications ThinApp à des machines et à des pools de postes de travail », page 242

Procédure

1 Téléchargez le logiciel ThinApp sur le site http://www.vmware.com/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 du Serveur de connexion View et à vos postes de travail distants et configurez le fichier et les autorisations de partage du dossier partagé afin d'accorder un droit d'accès en lecture aux ordinateurs du 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 si vous souhaitez attribuer les applications ThinApp à des machines ou à des pools de postes de travail.

   Si vous utilisez une convention de dénomination commune pour vos machines, vous pouvez utiliser les attributions de machine pour distribuer rapidement les applications à toutes les machines utilisant une convention de dénomination commune. Si vous organisez vos pools de poste de travail par type de service ou d'utilisateur, vous pouvez utiliser des attributions de pool de postes de travail pour distribuer rapidement les applications à des services ou à des utilisateurs spécifiques.

8 Dans View Administrator, sélectionnez les applications ThinApp à attribuer à vos machines ou pools de postes de travail et spécifiez le mode d'installation.

Option	Action
Diffusion en continu	Installe un raccourci vers l'application sur la machine. 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.
Complète	Installe l'application complète sur le système de fichiers local de la machine.

9 Dans View Administrator, vérifiez l'état d'installation des applications ThinApp.

Configuration de clients en mode kiosque

13

Vous pouvez configurer des clients sans assistance qui peuvent obtenir un accès à leurs postes de travail à partir de View.

Un client en mode Kiosque est un client léger ou un PC verrouillé qui exécute Horizon Client pour se connecter à une instance du Serveur de connexion View et lancer une session à distance. En général, les utilisateurs finaux n'ont pas besoin d'ouvrir une session pour accéder au périphérique client, même si le poste de travail distant peut nécessiter 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 utilise la fonctionnalité Authentification flexible dans View 4.5 et version ultérieure 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 afin qu'il obtienne un mot de passe généré automatiquement, vous pouvez exécuter Horizon 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 Horizon Client. Comme vous exécutez généralement Horizon Client à partir d'un script, et que le mot de passe apparaît en texte 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. Horizon Client dans View 4.5 et version ultérieure n'autorise pas la saisie manuelle de noms d'utilisateurs dans ces types de formats.

Il est recommandé d'utiliser des instances du 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 afin de 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.

- Informations d'identification des **Admins du domaine** ou des **Opérateurs de compte** dans Active Directory pour modifier les comptes des utilisateurs et des groupes dans un domaine.
- **Administrateurs**, **Administrateurs d'inventaire** ou un rôle équivalent afin d'utiliser View Administrator pour octroyer des postes de travail distants à des utilisateurs ou à des groupes.
- **Administrateurs** ou un rôle équivalent pour exécuter la commande `vdmadmin`.

Procédure

1 Préparer Active Directory et View pour les clients en mode Kiosque page 261

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 262

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 263

Si vous souhaitez créer un compte pour un client sur la base de son adresse MAC, vous pouvez utiliser Horizon Client pour détecter l'adresse MAC du périphérique client.

4 Ajout de comptes pour des clients en mode kiosque page 263

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 du 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 265

Vous pouvez utiliser la commande `vdmadmin` pour activer l'authentification de clients qui tentent de se connecter à leur poste de travail distant via une instance du Serveur de connexion View.

6 Vérifier la configuration de clients en mode kiosque page 266

Vous pouvez utiliser la commande `vdmadmin` pour afficher des informations sur des clients en mode kiosque et des instances du Serveur de connexion View qui sont configurées pour authentifier de tels clients.

7 Connecter des postes de travail distants à partir de clients en mode Kiosque page 267

Vous pouvez exécuter le 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 pour les 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 machine virtuelle dans un pool de postes de travail manuel. Vous pouvez également installer et configurer des applications sur le système d'exploitation invité.

3 Configurez le système d'exploitation invité afin que les clients ne soient pas verrouillés lorsqu'ils sont laissés sans assistance.

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 déverrouiller l'écran et afficher un message, vous pouvez configurer une application appropriée sur le système d'exploitation invité.

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 attribue un poste de travail distant de manière aléatoire à partir des pools auxquels un client est autorisé à accéder 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 `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 `Paramètres du logiciel` sous `Configuration ordinateur`.

6 Configurez les autres stratégies dont vous avez besoin pour optimiser et sécuriser les postes de travail distants des clients.

Par exemple, vous pouvez avoir besoin de remplacer les stratégies qui connectent des périphériques USB locaux au poste de travail distant lorsqu'il est lancé ou lorsque les périphériques sont branchés. Par défaut, Horizon Client pour Windows active ces stratégies 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 du Serveur de connexion View dans le groupe qui contient l'instance du Serveur de connexion View que les clients utiliseront pour se connecter à leur poste de travail distant.

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 du Serveur de connexion View 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 Serveur de connexion View. 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*	Specifies the distinguished name of the default organizational unit to which client accounts are added. For example: OU=kiosk-ou,DC=myorg,DC=com **Remarque** You cannot use the command to change the configuration of an organizational unit.

The command updates the default values for clients in the View Connection Server group.

Exemple : Setting Default Values for Cients in Kiosk Mode

Set the default values for the organizational unit, password expiry, and group membership of clients.

```
vdmadmin –Q –clientauth –setdefaults –ou "OU=kiosk–ou,DC=myorg,DC=com" –noexpirepassword –group
kc–grp
```

Suivant

Find out the MAC addresses of client devices that use their MAC address for authentication.

Afficher les adresses MAC de périphériques client

Si vous souhaitez créer un compte pour un client sur la base de son adresse MAC, vous pouvez utiliser Horizon Client pour détecter 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	Entrez **`C:\Program Files (x86)\VMware\VMware Horizon View Client\vmware-view.exe -printEnvironmentInfo`** Le client utilise l'instance du Serveur de connexion View par défaut que vous avez configurée pour lui. Si vous n'avez pas configuré de valeur par défaut, le client vous invite à en fournir une. 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 nom de domaine complet de l'instance du Serveur de connexion View que le 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 du 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 du Serveur de connexion View dans le groupe qui contient l'instance du Serveur de connexion View que les clients utiliseront pour se connecter à leur poste de travail distant.

Lorsque vous ajoutez un client en mode Kiosque, View 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 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 du 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***	Specifies the distinguished name of the organizational unit to which the client's account is added. For example: OU=kiosk-ou,DC=myorg,DC=com
`–password "`*password*`"`	Specifies an explicit password for the client's account.

The command creates a user account in Active Directory for the client in the specified domain and group (if any).

Exemple : Adding Accounts for Clients

Add an account for a client specified by its MAC address to the MYORG domain, using the default settings for the group kc-grp.

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid 00:10:db:ee:76:80 –group kc–grp
```

Add an account for a client specified by its MAC address to the MYORG domain, using an automatically generated password.

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid 00:10:db:ee:76:80 –genpassword
```

Add an account for a named client, and specify a password to be used with the client.

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid custom–Terminal21 –password "guest" –ou
"OU=kiosk–ou,DC=myorg,DC=com" –description "Terminal 21"
```

Add an account for a named client, using an automatically generated password.

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid custom–Kiosk11 –genpassword –ou "OU=kiosk–
ou,DC=myorg,DC=com" –description "Kiosk 11"
```

Suivant

Enable authentication of the 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 leur poste de travail distant via une instance du Serveur de connexion View.

Vous devez exécuter la commande `vdmadmin` sur l'une des instances du Serveur de connexion View dans le groupe qui contient l'instance du Serveur de connexion View que les clients utiliseront pour se connecter à leur poste de travail distant.

Même si vous activez l'authentification pour une instance individuelle du Serveur de connexion View, toutes les instances du Serveur de connexion View 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 Serveur de connexion View, toutes les instances du Serveur de connexion View activées peuvent authentifier le client.

Si vous prévoyez d'utiliser le mode kiosque avec un poste de travail View basé sur une session sur un hôte RDS, vous devez également ajouter le compte d'utilisateur au groupe Utilisateurs de postes de travail distants.

Procédure

1 Activez l'authentification de clients sur une instance du Serveur de connexion View.

```
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 du 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 du 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 `Unknown username or bad password`.
–s *connection_server*	Spécifie le nom NetBIOS de l'instance du Serveur de connexion View sur laquelle activer l'authentification de clients.

La commande active l'instance du Serveur de connexion View spécifiée pour authentifier des clients.

2 Si le poste de travail distant est fourni par un hôte Microsoft RDS, connectez-vous à l'hôte RDS et ajoutez le compte d'utilisateur au groupe Utilisateurs de postes de travail distants.

Par exemple, sur View Server, supposons que vous octroyez au compte d'utilisateur `custom–11` un poste de travail View basé sur une session sur un hôte RDS. Vous devez vous connecter à l'hôte RDS, puis ajouter l'utilisateur `custom–11` au groupe Utilisateurs de postes de travail distants en accédant à **Panneau de configuration > Système et sécurité > Système > Paramètres distants > Sélectionner des utilisateurs > Ajouter**.

Exemple : Activation de l'authentification de clients en mode kiosque

Activez l'authentification de clients pour l'instance du 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 des clients pour l'instance du Serveur de connexion View csvr-3, et demandez que les clients spécifient leurs mots de passe à Horizon 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 du Serveur de connexion View 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 du Serveur de connexion View qui sont configurées pour authentifier de tels clients.

Vous devez exécuter la commande `vdmadmin` sur l'une des instances du Serveur de connexion View dans le groupe qui contient l'instance du Serveur de connexion View que les clients utiliseront pour se connecter à leur poste de travail distant.

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 du Serveur de connexion View 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 ne nécessite pas qu'un utilisateur final ou un script d'application spécifie ce mot de passe dans Horizon 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 du 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
```

Suivant

Vérifiez que les clients peuvent se connecter à leur poste de travail distant.

Connecter des postes de travail distants à partir de clients en mode Kiosque

Vous pouvez exécuter le 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 Horizon Client sur un périphérique client déployé.

Remarque Sur un client Windows ou Mac, par défaut 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 distant. Sur tous les clients, 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	Entrez **C:\Program Files (x86)\VMware\VMware Horizon View Client\vmware-view.exe -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 nom de domaine complet de l'instance du Serveur de connexion View qu'Horizon Client utilisera pour se connecter à son poste de travail distant. Si vous ne spécifiez pas l'adresse IP ou le nom de domaine complet de l'instance du Serveur de connexion View que le client utilisera pour se connecter à son poste de travail distant, le client utilise l'instance par défaut du Serveur de connexion View 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 souhaitez pas qu'Horizon Client retente la connexion 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 nom de domaine complet de l'instance du Serveur de connexion View que le 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 le serveur authentifie le client kiosque et qu'un poste de travail distant est disponible, la commande démarre la session distante.

Exemple : Exécution d' Horizon Client sur des clients en mode Kiosque

Exécutez Horizon Client sur un client Windows dont le nom de compte est basé sur son adresse MAC et qui dispose d'un mot de passe généré automatiquement.

```
C:\Program Files (x86)\VMware\VMware Horizon View Client\vmware-view.exe -unattended -serverURL
consvr2.myorg.com
```

Exécutez Horizon Client sur un client Linux en utilisant un nom et un mot de passe attribués.

```
vmware-view -unattended -s 145.124.24.100 --once -u custom-Terminal21 -p "Secret1!"
```

Dépannage de View 14

Vous pouvez utiliser un grand nombre de procédures pour diagnostiquer et résoudre les problèmes que vous êtes susceptible de rencontrer dans View. 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.

Pour plus d'informations sur le dépannage des postes de travail et des pools de postes de travail, consultez le document *Configuration des postes de travail virtuels dans Horizon 7*.

Ce chapitre aborde les rubriques suivantes :

Contrôle de la santé du système

Vous pouvez utiliser le tableau de bord Intégrité du système dans View Administrator pour voir rapidement les problèmes pouvant affecter le fonctionnement de View ou l'accès à des postes de travail distants par des utilisateurs finaux.

Le tableau de bord Intégrité du système situé en haut à gauche de l'écran de View Administrator fournit un certain nombre de liens que vous pouvez utiliser pour afficher des rapports sur le fonctionnement de View :

Sessions	Fournit un lien vers l'écran Sessions qui affiche des informations sur l'état des sessions de poste de travail et d'applications distantes.
VM vCenter problématiques	Fournit un lien vers l'écran Machines qui affiche des informations sur les machines virtuelles vCenter, les hôtes RDS et autres machines que View a signalées comme problématiques.
Hôtes RDS problématiques	Fournit un lien vers l'onglet **Hôtes RDS** sur l'écran Machines qui affiche des informations sur les hôtes RDS que View a signalés comme problématiques.

Événements	Fournit des liens vers l'écran Events (Événements) filtré pour des événements d'erreur et pour des événements d'avertissement.
Intégrité du système	Fournit des liens vers l'écran 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 banques 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.

Surveiller les événements dans View

La base de données des événements stocke des informations sur les événements qui surviennent dans l'hôte ou le groupe Serveur de connexion View, Horizon 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 Events (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, reportez-vous au document *Intégration de View*.

En plus de surveiller 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. Reportez-vous à « Génération de messages du journal des événements de View au format Syslog à l'aide de l'option -I », page 291 et à « Configuration de la journalisation des événements pour des serveurs Syslog » dans le document *Installation de View*.

Prérequis

Créez et configurez la base de données des événements comme décrit dans le document *Installation de View*.

Procédure

1 Dans View Administrator, sélectionnez **Contrôle > Événements**.

2 (Facultatif) Dans la fenêtre Events (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'événements View

View signale des événements dès que l'état du système change ou rencontre un problème. Vous pouvez utiliser les informations dans les messages d'événement pour effectuer l'action appropriée.

Tableau 14-1 présente les types d'événements signalés par View.

Tableau 14-1. Types d'événements signalés par View

Type d'événement	Description
Audit Failure (Échec de l'audit) ou Audit Success (Succès de l'audit)	Signale l'échec ou la réussite d'une modification qu'un administrateur ou un utilisateur apporte au fonctionnement ou à la configuration de View.
Erreur	Signale l'échec d'une opération effectuée par View.
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 Audit Failure (Échec de l'audit), Error (Erreur) ou Warning (Avertissement). Vous n'avez pas à effectuer d'actions pour les événements Audit Success (Succès de l'audit) ou Information.

Collecte d'informations de diagnostic pour View

Vous pouvez collecter des informations de diagnostic pour aider le support technique de VMware à diagnostiquer et résoudre les problèmes avec View.

Vous pouvez collecter des informations de diagnostic pour divers composants de View. Le mode de collecte de ces informations varie en fonction du composant View.

- Créer un groupe DCT pour Horizon Agent page 273

  Pour aider le support technique de VMware à résoudre les problèmes d'Horizon 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 Horizon Client page 274

  Si vous rencontrez des problèmes lors de l'utilisation d'Horizon Client et que vous ne parvenez pas à les résoudre avec des techniques de dépannage réseau générales, vous pouvez enregistrer une copie des fichiers journaux et des informations de configuration.

- Collecter des informations de diagnostic pour View Composer à l'aide du script de support page 275

  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 le Serveur de connexion Horizon page 275

  Vous pouvez utiliser l'outil de support pour définir des niveaux de journalisation et générer des fichiers journaux pour le Serveur de connexion Horizon.

- Collecter des informations de diagnostic d'Horizon Agent, d'Horizon Client ou du Serveur de connexion Horizon à partir de la console page 276

  Si vous disposez d'un accès direct à la console, vous pouvez utiliser les scripts de prise en charge pour générer des fichiers journaux pour le Serveur de connexion, Horizon Client ou les postes de travail distants exécutant Horizon Agent. Ces informations aident le support technique de VMware à diagnostiquer des problèmes se produisant avec ces composants.

Créer un groupe DCT pour Horizon Agent

Pour aider le support technique de VMware à résoudre les problèmes d'Horizon 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 vous faciliter la tâche, vous pouvez utiliser la commande `vdmadmin` sur une instance de Serveur de connexion View pour demander un bundle DCT d'un poste de travail distant. Le groupe est renvoyé à Serveur de connexion View.

Vous pouvez également vous connecter à un poste de travail distant spécifique et exécuter une commande `support` qui crée le bundle DCT sur ce poste de travail. Si le Contrôle de compte d'utilisateur (UAC) est activé, vous devez obtenir le bundle 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	Connectez-vous à une instance standard ou réplica du Serveur de connexion View en tant qu'utilisateur disposant du rôle **Administrateurs**.
Sur le poste de travail distant	Ouvrez une session sur le poste de travail distant en tant qu'utilisateur disposant de privilèges administratifs.

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 distant	Passez au répertoire `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 : Utilisation de vdmadmin pour créer un fichier de groupe pour Horizon 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 Horizon Client

Si vous rencontrez des problèmes lors de l'utilisation d'Horizon Client et que vous ne parvenez pas à les résoudre avec des techniques de dépannage réseau générales, vous pouvez enregistrer une copie des fichiers journaux et des informations de configuration.

Avant d'enregistrer les informations de diagnostic et de contacter le support technique de VMware, essayez de résoudre les problèmes de connexion d'Horizon Client. Pour plus d'informations, reportez-vous à la section « Problèmes de connexion entre Horizon Client et le Serveur de connexion Horizon » dans le document *Configuration des postes de travail virtuels dans Horizon 7*.

Procédure

1 Dans Horizon Client, cliquez sur **Informations de support** ou, dans le menu du poste de travail distant, sélectionnez **Options > Informations de support**.

2 Dans la fenêtre Informations sur le 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, répondez aux invites en entrant les URL des instances du Serveur de connexion Horizon avec lesquelles vous voulez tester la configuration d'Horizon Client et, si nécessaire, en choisissant de générer les vidages de diagnostic des processus d'Horizon 7.

   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 le Serveur de connexion Horizon

Vous pouvez utiliser l'outil de support pour définir des niveaux de journalisation et générer des fichiers journaux pour le Serveur de connexion Horizon.

L'outil de support collecte des données de journalisation pour le Serveur de connexion. Ces informations aident le support technique de VMware à diagnostiquer des problèmes se produisant avec le Serveur de connexion. L'outil du support n'est pas prévu pour collecter des informations de diagnostic concernant Horizon Client ou Horizon Agent. À la place, vous devez utiliser le script de support. Reportez-vous à la section « Collecter des informations de diagnostic d'Horizon Agent, d'Horizon Client ou du Serveur de connexion Horizon à partir de la console », page 276.

Prérequis

Connectez-vous à une instance standard ou réplica du Serveur de connexion en tant qu'utilisateur disposant du rôle **Administrateurs**.

Procédure

1 Sélectionnez **Démarrer > Tous les programmes > VMware > Définir les niveaux de journal du Serveur de connexion View**.

2 Dans la zone de texte **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 de journalisation normal.
2	Sélectionne un niveau de débogage de journalisation (par défaut).
3	Sélectionne la journalisation complète.

Le système démarre l'enregistrement des informations de journal avec le niveau de détail que vous avez sélectionné.

3 Après avoir collecté suffisamment d'informations sur le comportement du Serveur de connexion, sélectionnez **Démarrer > Tous les programmes > VMware > Générer un bundle de journaux du Serveur de connexion View**.

L'outil de support écrit les fichiers journaux dans un dossier appelé `vdm-sdct` sur le poste de travail de l'instance du Serveur de connexion.

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 d' Horizon Agent , d'Horizon Client ou du Serveur de connexion Horizon à partir de la console

Si vous disposez d'un accès direct à la console, vous pouvez utiliser les scripts de prise en charge pour générer des fichiers journaux pour le Serveur de connexion, Horizon Client ou les postes de travail distants exécutant Horizon 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. Vous devez vous connecter en tant qu'utilisateur disposant des privilèges d'administrateur.

- Pour Horizon Agent, connectez-vous à la machine virtuelle sur laquelle Horizon Agent est installé.
- Pour Horizon Client, connectez-vous au système sur lequel est installé Horizon Client.
- Pour le Serveur de connexion, ouvrez une session sur l'hôte du Serveur de connexion.

Procédure

1 Ouvrez une fenêtre d'invite de commande et accédez au répertoire correspondant au composant Horizon 7 pour lequel vous souhaitez collecter les informations de diagnostic.

Option	Description
Horizon Agent	Passez au répertoire `C:\Program Files\VMware View\Agent\DCT`.
Horizon 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 de journalisation normal.
2	Sélectionne un niveau de débogage de journalisation (par défaut).
3	Sélectionne la journalisation complète.
4	Sélectionne la journalisation des informations pour PCoIP (Horizon Agent et Horizon Client uniquement).
5	Sélectionne la journalisation de débogage pour PCoIP (Horizon Agent et Horizon Client uniquement).
6	Sélectionne la journalisation des informations pour les canaux virtuels (Horizon Agent et Horizon Client uniquement).
7	Sélectionne la journalisation de débogage pour les canaux virtuels (Horizon Agent et Horizon Client uniquement).
8	Sélectionne la journalisation du suivi pour les canaux virtuels (Horizon Agent et Horizon 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 **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`.

Dépannage 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.
- Horizon Client ne peut pas se connecter à View. Le message d'erreur suivant apparaît : `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 conserver le serveur de sécurité dans votre environnement View, procédez comme suit :

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

2 Dans l'onglet **Serveurs de sécurité**, sélectionnez un serveur de sécurité, sélectionnez **Préparer la mise à niveau ou la réinstallation** dans le menu déroulant **Plus de commandes**, puis cliquez sur **OK**.

3 Dans l'onglet **Serveurs de connexion**, sélectionnez l'instance du Serveur de connexion View que vous souhaitez associer au serveur de sécurité, sélectionnez **Spécifier un mot de passe de couplage de serveur de sécurité** dans le menu déroulant **Plus de commandes**, tapez un mot de passe, puis 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 du Serveur de connexion View utilisée pour des connexions Horizon Client sécurisées peut s'afficher en rouge dans View Administrator si la vérification de la révocation de 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 du serveur View inclut le message suivant : `Le certificat du serveur ne peut pas être vérifié`.

Cause

La vérification de la révocation des certificats peut échouer si votre organisation 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 Serveur de connexion VMware Horizon 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 organisation.

5 Configurez les paramètres proxy.

   Par exemple, à la suite de 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 Horizon 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 62.

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.

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, reportez-vous aux articles proposés sur le site Web de la base de connaissances VMware :

http://kb.vmware.com/selfservice/microsites/microsite.do

Utilisation de la commande vdmadmin

15

Vous pouvez utiliser l'interface de ligne de commande `vdmadmin` pour effectuer diverses tâches d'administration sur une instance du 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, dans des applets de commande View et dans `vdmadmin`, reportez-vous au document *Intégration de View*.

- Génération de messages du journal des événements de View au format Syslog à l'aide de l'option -I page 291

  Vous pouvez utiliser la commande `vdmadmin` avec l'option `–I` pour enregistrer les messages d'événements de View au format `Syslog` dans les fichiers journaux des événements. De nombreux produits d'analyse tiers requièrent des données `Syslog` de fichier plat comme entrée pour leurs opérations d'analyse.

- Attribution de machines dédiées à l'aide de l'option -L page 293

  Vous pouvez utiliser l'option `–L` de la commande `vdmadmin` pour attribuer aux utilisateurs des machines provenant d'un pool dédié.

- Affichage d'informations sur les machines à l'aide de l'option -M page 294

  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 295

  Vous pouvez utiliser la commande `vdmadmin` avec l'option `–M` pour marquer une machine virtuelle de clone lié pour la récupération d'espace disque. Horizon 7 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 Horizon Administrator.

- Configuration de filtres de domaine à l'aide de l'option -N page 296

  Vous pouvez utiliser la commande `vdmadmin` avec l'option `–N` pour contrôler les domaines que View rend disponibles aux utilisateurs finaux.

- Configuration de filtres de domaine page 298

  Vous pouvez configurer des filtres de domaine pour limiter les domaines qu'une instance du Serveur de connexion View ou un serveur de sécurité rend disponibles aux utilisateurs finaux.

- Affichage des machines et des stratégies d'utilisateurs non autorisés à l'aide des options -O et -P page 302

  Vous pouvez utiliser la commande `vdmadmin` avec les options `–O` et `–P` pour afficher les machines virtuelles et les stratégies qui sont attribuées 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 304

  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'une machine à l'aide de l'option -R page 308

  Vous pouvez utiliser la commande `vdmadmin` avec l'option `–R` pour connaître l'attribution initiale d'une machine virtuelle gérée. Par exemple, en cas de perte de données LDAP, vous pouvez avoir besoin de ces informations pour pouvoir réattribuer des machines virtuelles 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 308

  Vous pouvez utiliser la commande `vdmadmin` avec l'option `–S` pour supprimer l'entrée d'une instance du Serveur de connexion View ou du serveur de sécurité de la configuration de View.

- Fournir des informations d'identification secondaires à des administrateurs à l'aide de l'option -T page 309

  Vous pouvez utiliser la commande `vdmadmin` avec l'option `–T` pour fournir des informations d'identification secondaires Active Directory à des utilisateurs administrateurs.

- Affichage d'informations sur les utilisateurs à l'aide de l'option -U page 311

  Vous pouvez utiliser la commande `vdmadmin` avec l'option `–U` pour afficher des informations détaillées sur les utilisateurs.

- Déverrouillage ou verrouillage de machines virtuelles à l'aide de l'option -V page 312

  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 313

  Vous pouvez utiliser la commande `vdmadmin` avec l'option `–X` pour détecter et résoudre les entrées LDAP en collision sur des instances du Serveur de connexion View 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 283

  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 284

  Certaines options de la commande `vdmadmin` vous permettent de spécifier le format des informations de sortie.

- Options de la commande vdmadmin page 284

  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. Reportez-vous à la section Chapitre 6, « Configuration d'administration déléguée basée sur des rôles », page 111.

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 entrer le mot de passe, et la commande vdmadmin ne conserve pas les mots de passe sensibles dans l'historique des commandes sur la ligne de commande.

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 15-1 montre les options que certaines options de la commande vdmadmin fournissent pour la mise en forme du texte de sortie.

Tableau 15-1. 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 15-2 montre les options de commande que vous pouvez utiliser avec la commande vdmadmin pour contrôler et vérifier le fonctionnement de View.

Tableau 15-2. Options de la commande Vdmadmin

Option	Description
–A	Administre les informations qu'Horizon Agent enregistre dans ses fichiers journaux. Reportez-vous à la section « Configuration de la journalisation dans Horizon Agent à l'aide de l'option -A », page 285. Remplace l'adresse IP signalée par Horizon Agent. Reportez-vous à la section « Remplacement d'adresses IP à l'aide de l'option -A », page 287.
–C	Définit le nom d'un groupe Serveur de connexion View. Reportez-vous à la section « Définition du nom d'un groupe du Serveur de connexion View à l'aide de l'option -C », page 288.
–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 289.
–H	Affiche des informations sur la santé de services View. Reportez-vous à la section « Liste et affichage de moniteurs d'intégrité à l'aide de l'option -H », page 289.
–I	Génère des rapports sur le fonctionnement de View. Reportez-vous à la section « Liste et affichage de rapports sur le fonctionnement de View à l'aide de l'option -I », page 290.
–L	Affecte un poste de travail dédié à un utilisateur ou supprime une affectation. Reportez-vous à la section « Attribution de machines dédiées à l'aide de l'option -L », page 293.
–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 294.

Tableau 15-2. Options de la commande Vdmadmin (suite)

Option	Description
–N	Configure les domaines qu'une instance ou un groupe du Serveur de connexion View rend disponibles dans Horizon Client. Reportez-vous à la section « Configuration de filtres de domaine à l'aide de l'option -N », page 296.
–O	Affiche les postes de travail distants attribués à des utilisateurs qui ne sont plus autorisés à y accéder. Reportez-vous à la section « Affichage des machines et des stratégies d'utilisateurs non autorisés à l'aide des options -O et -P », page 302.
–P	Affiche les stratégies utilisateur associées aux postes de travail distants d'utilisateurs non autorisés. Reportez-vous à la section « Affichage des machines et des stratégies d'utilisateurs non autorisés à l'aide des options -O et -P », page 302.
–Q	Configure le compte dans un compte Active Directory et la configuration de View 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 304.
–R	Signale le premier utilisateur ayant accédé à un poste de travail distant. Reportez-vous à la section « Affichage du premier utilisateur d'une machine à l'aide de l'option -R », page 308.
–S	Supprime de la configuration de View une entrée de configuration correspondant à une instance du Serveur de connexion View. 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 308.
–T	Fournit les informations d'identification secondaires Active Directory à des utilisateurs administrateurs. Reportez-vous à la section « Fournir des informations d'identification secondaires à des administrateurs à l'aide de l'option -T », page 309.
–U	Affiche des informations sur un utilisateur, notamment ses droits d'accès de postes de travail distants, ses attributions ThinApp, et ses rôles d'administrateur. Reportez-vous à la section « Affichage d'informations sur les utilisateurs à l'aide de l'option -U », page 311.
–V	Déverrouille ou verrouille des machines virtuelles. Reportez-vous à la section « Déverrouillage ou verrouillage de machines virtuelles à l'aide de l'option -V », page 312.
–X	Détecte et résout les entrées LDAP en double dans des instances du Serveur de connexion View répliquées. Reportez-vous à la section « Détection et résolution des collisions d'entrée LDAP à l'aide de l'option -X », page 313.

Configuration de la journalisation dans Horizon Agent à l'aide de l'option -A

Vous pouvez utiliser la commande `vdmadmin` avec l'option –A pour configurer la journalisation par Horizon 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 d'Horizon Agent, vous pouvez créer un groupe DCT (Data Collection Tool). Vous pouvez également modifier le niveau de journalisation, afficher la version et l'état d'Horizon Agent et enregistrer des fichiers journaux individuels sur votre disque local.

Options

Tableau 15-3 montre les options que vous pouvez spécifier pour configurer la journalisation dans Horizon Agent.

Tableau 15-3. Options pour configurer la journalisation dans Horizon 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 d'Horizon Agent.
`-getstatus`	Affiche l'état d'Horizon Agent.
`-getversion`	Affiche la version d'Horizon Agent.
`-list`	Répertorie les fichiers journaux pour Horizon Agent.
`-m` *machine*	Spécifie la machine dans un pool de postes de travail.
`-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 d'Horizon 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 d'Horizon 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 d'Horizon 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 d'Horizon 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 d'Horizon 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 d'Horizon Agent pour la machine machine1 dans le pool de postes de travail dtpool2.

```
vdmadmin -A -d dtpool2 -m machine1 -getversion
```

Affichez l'état d'Horizon 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 Horizon 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

Horizon Agent signale l'adresse IP découverte de la machine sur laquelle il est exécuté à l'instance du Serveur de connexion View. Dans des configurations sécurisées où l'instance du Serveur de connexion View ne peut pas approuver la valeur signalée par Horizon Agent, vous pouvez remplacer la valeur fournie par Horizon Agent et spécifier l'adresse IP que la machine gérée devrait utiliser. Si l'adresse d'une machine signalée par Horizon Agent ne correspond pas à l'adresse définie, vous ne pouvez pas utiliser Horizon Client pour accéder à la machine.

Options

Tableau 15-4 montre les options que vous pouvez spécifier pour remplacer des adresses IP.

Tableau 15-4. 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 du 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 du 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. 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 de 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 View*.

Options

L'option `–c` spécifie le nom du groupe de 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 du 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 l'option `–H` de la commande `vdmadmin` pour répertorier les moniteurs de santé existants, pour surveiller les instances des composants de View et pour afficher les détails d'un moniteur de santé ou d'une instance de moniteur 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 15-5 indique les moniteurs de santé utilisés par View pour surveiller la santé de ses composants.

Tableau 15-5. Moniteurs d'intégrité

Moniteur	Description
CBMonitor	Contrôle l'intégrité des instances du Serveur de connexion View.
DBMonitor	Contrôle l'intégrité de la base de données des événements.

Tableau 15-5. Moniteurs d'intégrité (suite)

Moniteur	Description
DomainMonitor	Contrôle l'intégrité du domaine local et de tous les domaines approuvés de l'hôte du Serveur de connexion View.
SGMonitor	Contrôle l'intégrité des services de passerelle de sécurité et des serveurs de sécurité.
VCMonitor	Contrôle l'intégrité des serveurs vCenter.

Si un composant dispose de plusieurs instances, View crée une instance de moniteur distincte pour surveiller 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 15-6 montre les options que vous pouvez spécifier pour répertorier et afficher des moniteurs d'intégrité.

Tableau 15-6. 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 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 et pour afficher les résultats de l'exécution 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 a enregistrées pour un rapport et une vue spécifiés.

Vous pouvez également utiliser la commande `vdmadmin` avec l'option `-I` pour générer les messages de journaux de View au format `syslog`. Reportez-vous à la section « Génération de messages du journal des événements de View au format Syslog à l'aide de l'option -I », page 291.

Options

Tableau 15-7 montre les options que vous pouvez spécifier pour répertorier et afficher des rapports et des vues.

Tableau 15-7. 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 du journal des événements de View au format Syslog à l'aide de l'option -I

Vous pouvez utiliser la commande `vdmadmin` avec l'option `-I` pour enregistrer les messages d'événements de View au format `Syslog` dans les fichiers journaux 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 les messages du journal des événements de View au format `Syslog`. Dans un fichier `Syslog`, les messages du journal des événements de View sont formatés en paires clé-valeur, ce qui rend la journalisation des données accessible aux logiciels 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 à l'aide de l'option -I », page 290.

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 à un serveur `Syslog` est prise en charge par View 5.2 ou version ultérieure. Reportez-vous à la section « Configuration de la journalisation des événements pour des serveurs Syslog » du document *Installation de View*.

Tableau 15-8. 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 les événements de 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`.
`–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

Désactivez la génération d'événements de View au format `Syslog`.

```
vdmadmin –I –eventSyslog –disable
```

Dirigez la sortie `Syslog` des événements de View vers le système local uniquement.

```
vdmadmin –I –eventSyslog –enable –localOnly
```

Dirigez la sortie `Syslog` des événements de View vers un chemin d'accès spécifié.

```
vdmadmin –I –eventSyslog –enable –path path
```

Dirigez la sortie `Syslog` des événements de View vers un chemin d'accès spécifié nécessitant l'accès par un utilisateur de domaine autorisé.

```
vdmadmin –I –eventSyslog –enable –path \\logserver\share\ViewEvents –user mydomain\myuser
 –password mypassword
```

Attribution de machines dédiées à l'aide de l'option -L

Vous pouvez utiliser l'option –L de la commande vdmadmin pour attribuer aux utilisateurs des machines provenant d'un pool dédié.

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 attribue des machines aux utilisateurs lorsqu'ils se connectent pour la première fois à un pool de postes de travail dédié. Dans certains cas, vous pouvez souhaiter pré-attribuer des machines aux utilisateurs. Par exemple, vous voulez peut-être préparer leurs environnements système avant leur connexion initiale. Dès qu'un utilisateur se connecte à un poste de travail distant attribué par View à partir d'un pool dédié, la machine virtuelle qui héberge le poste de travail reste attribuée à l'utilisateur pendant toute la durée de sa vie. Vous pouvez attribuer un utilisateur à un seule machine d'un pool dédié.

Vous pouvez attribuer une machine à n'importe quel utilisateur autorisé. Vous pouvez effectuer cette opération lorsque vous récupérez des données View LDAP perdues sur une instance du Serveur de connexion View, ou pour modifier le propriétaire d'une machine virtuelle.

Dès qu'un utilisateur se connecte à un poste de travail distant attribué par View à partir d'un pool dédié, ce poste de travail distant reste attribué à l'utilisateur pendant toute la durée de la vie de la machine virtuelle hébergeant le poste de travail. Vous pouvez souhaiter supprimer l'attribution d'une machine à un utilisateur qui a quitté l'organisation et qui n'a plus besoin d'accéder au poste de travail ou qui utilisera un poste de travail d'un autre pool. 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 15-9 montre les options que vous pouvez spécifier pour affecter un poste de travail à un utilisateur ou pour supprimer une affectation.

Tableau 15-9. Options pour l'affectation de postes de travail dédiés

Option	Description
–d *desktop*	Spécifie le nom du pool de postes de travail.
–m *machine*	Spécifie le nom de la machine virtuelle qui héberge le poste de travail distant.
–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 la machine virtuelle ou l'ordinateur physique sous-jacent d'un poste de travail distant.

- 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 `Connecté` ou `Déconnecté`, 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.
- 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 15-10 montre les options que vous pouvez utiliser pour spécifier la machine pour laquelle vous voulez afficher des détails.

Tableau 15-10. Options pour l'affichage d'informations sur les machines

Option	Description
`–d` *desktop*	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 du poste de travail figurant dans le pool dtpool2 qui est attribué 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. Horizon 7 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 Horizon 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 qu'Horizon 7 utilise vCenter Server et ESXi version 5.1 ou ultérieure.
- 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 Horizon 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 Horizon 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 l'espace disque sur des clones liés View Composer » dans le document *Configuration des postes de travail virtuels dans Horizon 7*.
- 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 les durées d'interruption de Storage Accelerator et de récupération d'espace des clones liés View Composer » dans le document *Configuration des postes de travail virtuels dans Horizon 7*.

Options

Tableau 15-11. Options de récupération d'espace disque sur des machines virtuelles

Option	Description
`–d` *desktop*	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 rend disponibles aux 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 15-12 montre les options que vous pouvez spécifier pour configurer des filtres de domaine.

Tableau 15-12. 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 du Serveur de connexion View ou pour le groupe Serveur de connexion View.
`-list -active`	Affiche les domaines disponibles pour l'instance du Serveur de connexion View sur laquelle vous exécutez la commande.
`-remove`	Supprime un domaine d'une liste.
`-removeall`	Supprime tous les domaines d'une liste.
`-s` *connsvr*	Spécifie que l'opération s'applique aux filtres de domaine sur une instance du Serveur de connexion View. Vous pouvez spécifier l'instance du Serveur de connexion View 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 du Serveur de connexion View 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 du Serveur de connexion View csvr1.

```
vdmadmin -N -domains -search -domain FARDOM -add -s csvr1
```

Ajoutez le domaine NEARDOM à la liste d'exclusion pour un groupe Serveur de connexion View.

```
vdmadmin -N -domains -exclude -domain NEARDOM -add
```

Affichez la configuration de recherche de domaine sur les deux instances du Serveur de connexion View 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 limite la recherche de domaine sur chaque hôte du Serveur de connexion View du groupe pour exclure les domaines FARDOM et DEPTX. Les caractères (*) en regard de la liste d'exclusion de CONSVR-1 indiquent que View exclut le domaine YOURDOM des résultats de la recherche de domaine 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 sur l'instance du Serveur de connexion View.

```
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 Serveur de connexion View.

```
vdmadmin -N -domains -exclude -domain NEARDOM -remove
```

Supprimez tous les domaines de la liste d'inclusion pour l'instance du Serveur de connexion View 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 du Serveur de connexion View ou un serveur de sécurité rend disponibles aux utilisateurs finaux.

View détermine les domaines qui sont accessibles en traversant des relations d'approbation, en commençant par le domaine dans lequel réside une instance du Serveur de connexion View ou un serveur de sécurité. Pour un petit ensemble de domaines bien connectés, View peut déterminer rapidement une liste complète de domaines, mais le temps que prend cette opération augmente au fur et à mesure que le nombre de domaines augmente ou que la connectivité entre les domaines diminue. View 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 distants.

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 du Serveur de connexion View 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 du Serveur de connexion View sur laquelle vous avez défini cette clé.

Tableau 15-13 montre les types de listes de domaines que vous pouvez spécifier pour configurer le filtrage de domaine.

Tableau 15-13. Types de liste de domaines

Type de liste de domaines	Description
Liste d'exclusion de recherche	Spécifie les domaines que View 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 exclut des résultats d'une recherche de domaines. Vous ne pouvez pas exclure le domaine principal.
Liste d'inclusion	Spécifie les domaines que View 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 sélectionne la première liste d'exclusion ou d'inclusion non vide dans cet ordre.

1 Liste d'exclusion configurée pour l'instance du Serveur de connexion View.

2 Liste d'exclusion configurée pour le groupe Serveur de connexion View.

3 Liste d'inclusion configurée pour l'instance du Serveur de connexion View.

4 Liste d'inclusion configurée pour le groupe Serveur de connexion View.

View 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 accessible actuellement, View n'inclut pas ce domaine dans la liste de domaines actifs.

Vous ne pouvez pas exclure le domaine principal auquel une instance du Serveur de connexion View 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 n'exclut pas des résultats d'une recherche de domaine. Tous les autres domaines sont supprimés à l'exception du domaine principal.

Une instance du Serveur de connexion View 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 du Serveur de connexion View.

```
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 du Serveur de connexion View 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 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 exclut des résultats d'une recherche de domaine.

Un groupe de deux instances du Serveur de connexion View, 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 Serveur de connexion View dans le domaine MYDOM.

Affichez les domaines actuellement actifs d'un membre du groupe Serveur de connexion View.

```
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 d'Horizon Client, excluez le domaine FARDOM des recherches effectuées par le groupe Serveur de connexion View.

```
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 du Serveur de connexion View 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 limite la recherche de domaine sur chaque hôte du Serveur de connexion View du groupe pour exclure les domaines FARDOM et DEPTX. Les caractères (*) en regard de la liste d'exclusion de CONSVR-1 indiquent que View exclut le domaine YOURDOM des résultats de la recherche de domaine 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 machines et des stratégies 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 machines virtuelles et les stratégies qui sont attribuées 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 le droit d'accès d'un utilisateur à une machine virtuelle persistante ou à un système physique, l'attribution du poste de travail distant associé 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 le droit d'accès, l'utilisateur peut continuer à utiliser la même machine virtuelle que précédemment. Si un utilisateur a quitté l'entreprise, les autres utilisateurs ne peuvent pas accéder à la machine virtuelle, et celle-ci est alors considérée comme étant orpheline. Vous voulez peut-être aussi examiner des règles qui sont affectées à des utilisateurs non autorisés.

Options

Tableau 15-14 montre les options que vous pouvez spécifier pour afficher les machines virtuelles et les stratégies d'utilisateurs non autorisés.

Tableau 15-14. Options pour l'affichage des machines et des stratégies d'utilisateurs non autorisés

Option	Description
`-ld`	Classe les entrées de sortie par machine.
`-lu`	Classe les entrées de sortie par utilisateur.

Tableau 15-14. Options pour l'affichage des machines et des stratégies d'utilisateurs non autorisés (suite)

Option	Description
`-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 15-15 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 15-15. Feuilles de style XSL

Nom du fichier de feuille de style	Description
`unentitled-machines.xsl`	Transforme des rapports contenant une liste de machines virtuelles non autorisées, groupées par utilisateur ou par système, et qui sont actuellement attribuées à un utilisateur. Il s'agit de la feuille de style par défaut.
`unentitled-policies.xsl`	Transforme des rapports contenant une liste de machines virtuelles disposant de stratégies de niveau utilisateur appliquées à des utilisateurs non autorisés.

Exemples

Affichez les machines virtuelles qui sont attribuées à des utilisateurs non autorisés, groupées par machine virtuelle au format de texte.

```
vdmadmin -O -ld
```

Affichez des machines virtuelles attribuées à des utilisateurs non autorisés, groupées par utilisateur, au format XML en utilisant des 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 stratégies d'utilisateur associées à des machines virtuelles d'utilisateurs non autorisés, groupées par poste de travail, au format XML en utilisant des 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 du Serveur de connexion View dans le groupe qui contient l'instance du Serveur de connexion View que les clients utilisent pour se connecter à leur poste de travail distant.

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 du Serveur de connexion View dans un groupe.

Lorsque vous ajoutez un client en mode Kiosque, View 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 du 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 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 du 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 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 du 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 pourront pas se connecter à leur poste de travail distant.

Même si vous activez ou désactivez l'authentification pour une instance individuelle du Serveur de connexion View, toutes les instances du 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 du 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 du 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 du 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 `Unknown username or bad password`.

Options

Tableau 15-16 montre les options que vous pouvez spécifier pour configurer des clients en mode kiosque.

Tableau 15-16. 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'authentication 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 du 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 du 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.

Tableau 15-16. Options pour la configuration de clients en mode kiosque (suite)

Option	Description
`–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.
`–list`	Affiche des informations sur les clients en mode kiosque et sur les instances du 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*	Specifies the distinguished name of the organizational unit to which client accounts are added. For example: OU=kiosk-ou,DC=myorg,DC=com **Remarque** You cannot use the `–setdefaults` option to change the configuration of an organizational unit.
`–password` "*password*"	Specifies an explicit password for the client's account.
`–remove`	Removes the account for a client in kiosk mode.
`–removeall`	Removes the accounts of all clients in kiosk mode.
`–requirepassword`	Specifies that clients in kiosk mode must provide passwords. View will not accept generated passwords for new connections.
`–s` *connection_server*	Specifies the NetBIOS name of the View Connection Server instance on which to enable or disable the authentication of clients in kiosk mode.
`–setdefaults`	Sets the default values that are used for adding client accounts.
`–update`	Updates an account for a client in kiosk mode.

Examples

Set the default values for the organizational unit, password expiry, and group membership of clients.

```
vdmadmin –Q –clientauth –setdefaults –ou "OU=kiosk–ou,DC=myorg,DC=com" –noexpirepassword –group kc–grp
```

Get the current default values for clients in plain text format.

```
vdmadmin –Q –clientauth –getdefaults
```

Get the current default values for clients in XML format.

```
vdmadmin –Q –clientauth –getdefaults –xml
```

Add an account for a client specified by its MAC address to the MYORG domain, and use the default settings for the group kc-grp.

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid 00:10:db:ee:76:80 –group kc–grp
```

Add an account for a client specified by its MAC address to the MYORG domain, and use an automatically generated password.

```
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
```

Add an account for a named client, and specify a password to be used with the client.

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid custom–Terminal21 –password "guest" –ou
"OU=kiosk–ou,DC=myorg,DC=com" –description "Terminal 21"
```

Update an account for a client, specifying a new password and descriptive text.

```
vdmadmin –Q –clientauth –update –domain MYORG –clientid custom–Terminal21 –password "Secret1!" –
description "Foyer Entry Workstation"
```

Remove the account for a kiosk client specified by its MAC address from the MYORG domain.

```
vdmadmin –Q –clientauth –remove –domain MYORG –clientid 00:10:db:ee:54:12
```

Remove the accounts of all clients without prompting to confirm the removal.

```
vdmadmin –Q –clientauth –removeall –force
```

Enable authentication of clients for the View Connection Server instance csvr-2. Clients with automatically generated passwords can authenticate themselves without providing a password.

```
vdmadmin –Q –enable –s csvr–2
```

Enable authentication of clients for the View Connection Server instance csvr-3, and require that the clients specify their passwords to Horizon Client. Clients with automatically generated passwords cannot authenticate themselves.

```
vdmadmin –Q –enable –s csvr–3 –requirepassword
```

Disable authentication of clients for the View Connection Server instance csvr-1.

```
vdmadmin –Q –disable –s csvr–1
```

Display information about clients in text format. Client cm-00_0c_29_0d_a3_e6 has an automatically generated password, and does not require an end user or an application script to specify this password to Horizon Client. Client cm-00_22_19_12_6d_cf has an explicitly specified password, and requires the end user to provide this. The View Connection Server instance CONSVR2 accepts authentication requests from clients with automatically generated passwords. CONSVR1 does not accept authentication requests from clients in kiosk mode.

```
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'une machine à l'aide de l'option -R

Vous pouvez utiliser la commande `vdmadmin` avec l'option `–R` pour connaître l'attribution initiale d'une machine virtuelle gérée. Par exemple, en cas de perte de données LDAP, vous pouvez avoir besoin de ces informations pour pouvoir réattribuer des machines virtuelles à des utilisateurs.

Remarque La commande `vdmadmin` avec l'option `–R` ne fonctionne que sur les machines virtuelles avec une version antérieure à View Agent 5.1. Sur des machines virtuelles qui exécutent View Agent 5.1 et versions ultérieures et Horizon Agent 7.0 et versions ultérieures, cette option ne fonctionne pas. Pour localiser le premier utilisateur d'une machine virtuelle, utilisez la base de données Événements pour déterminer quels utilisateurs sont connectés sur la machine.

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 être connecté en tant qu'utilisateur disposant du rôle **Administrateur**.

Options

L'option `–i` spécifie l'adresse IP de la machine virtuelle.

Exemples

Afficher le premier utilisateur qui a eu accès à la machine virtuelle 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 du Serveur de connexion View ou du serveur de sécurité de la configuration de View.

Syntaxe

```
vdmadmin –S [–b authentication_arguments] –r –s server
```

Notes d'utilisation

Pour garantir une disponibilité élevée, View vous permet de configurer une ou plusieurs instances réplicas du Serveur de connexion View dans un groupe Serveur de connexion View. Si vous désactivez une instance du Serveur de connexion View dans un groupe, l'entrée du serveur persiste dans la configuration de View.

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 Add or Remove Programs (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 du Serveur de connexion View dans le groupe d'origine avant d'effectuer la réinstallation. Cela évite aux instances réinstallées du 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 du Serveur de connexion View connsvr3.

```
vdmadmin –S –r –s connsvr3
```

Fournir des informations d'identification secondaires à des administrateurs à l'aide de l'option -T

Vous pouvez utiliser la commande `vdmadmin` avec l'option –T pour fournir des informations d'identification secondaires Active Directory à des utilisateurs administrateurs.

Syntaxe

```
vdmadmin –T [–b authentication_arguments] –domainauth
 {–add | –update | –remove | –removeall | –list} –owner domain\user –user domain\user [–password
password]
```

Notes d'utilisation

Si vos utilisateurs et groupes se trouvent dans un domaine avec une relation de confiance unidirectionnelle avec le domaine du Serveur de connexion View, vous devez fournir des informations d'identification secondaires aux utilisateurs administrateurs dans View Administrator. Les administrateurs doivent disposer d'informations d'identification secondaires pour pouvoir accéder aux domaines approuvés unidirectionnels. Un domaine approuvé unidirectionnel peut être un domaine externe ou un domaine dans une approbation de forêt transitive.

Les informations d'identification secondaires sont requises uniquement pour les sessions View Administrator, pas pour les sessions de poste de travail ou d'application des utilisateurs finaux. Seuls les utilisateurs administrateurs requièrent des informations d'identification secondaires.

La commande `vdmadmin` vous permet de configurer des informations d'identification secondaires pour chaque utilisateur. Vous ne pouvez pas configurer des informations d'identification secondaires spécifiées globalement.

En général, pour une approbation de forêt, vous configurez des informations d'identification secondaires uniquement pour le domaine racine de forêt. Le Serveur de connexion View peut ensuite énumérer les domaines enfants dans l'approbation de forêt.

Les vérifications des heures de verrouillage, de désactivation et d'ouverture de session du compte Active Directory peuvent être effectuées uniquement lorsqu'un utilisateur dans un domaine approuvé unidirectionnel se connecte pour la première fois.

L'administration PowerShell et l'authentification par carte à puce des utilisateurs ne sont pas prises en charge dans les domaines approuvés unidirectionnels. L'authentification SAML des utilisateurs dans des domaines approuvés unidirectionnels n'est pas prise en charge.

Les comptes d'informations d'identification secondaires requièrent les autorisations suivantes. Un compte d'utilisateur standard doit avoir ces autorisations par défaut.

- Lister le contenu
- Lire toutes les propriétés
- Autorisations de lecture
- Lire tokenGroupsGlobalAndUniversal (sous-entendu par Lire toutes les propriétés)

Options

Tableau 15-17. Options pour fournir des informations d'identification secondaires

Option	Description
`-add`	Ajoute des informations d'identification secondaires pour le compte du propriétaire. Une ouverture de session Windows est effectuée pour vérifier que les informations d'identification spécifiées sont valides. Une entité de sécurité externe est créée pour l'utilisateur dans View LDAP.
`-update`	Met à jour des informations d'identification secondaires pour le compte du propriétaire. Une ouverture de session Windows est effectuée pour vérifier que les informations d'identification mises à jour sont valides.
`-list`	Affiche les informations d'identification de sécurité pour le compte du propriétaire. Les mots de passe ne sont pas affichés.
`-remove`	Supprime des informations d'identification de sécurité du compte du propriétaire.
`-removeall`	Supprime toutes les informations d'identification de sécurité du compte du propriétaire.

Exemples

Ajoutez des informations d'identification secondaires pour le compte du propriétaire spécifié. Une ouverture de session Windows est effectuée pour vérifier que les informations d'identification spécifiées sont valides.

```
vdmadmin -T -domainauth -add -owner domain\user -user domain\user -password password
```

Mettez à jour des informations d'identification secondaires pour le compte du propriétaire spécifié. Une ouverture de session Windows est effectuée pour vérifier que les informations d'identification mises à jour sont valides.

```
vdmadmin -T -domainauth -update -owner domain\user -user domain\user -password password
```

Supprimez des informations d'identification secondaires pour le compte du propriétaire spécifié.

```
vdmadmin –T –domainauth –remove –owner domain\user –user domain\user
```

Supprimez toutes les informations d'identification secondaires pour le compte du propriétaire spécifié.

```
vdmadmin –T –domainauth –removeall –owner domain\user
```

Affichez toutes les informations d'identification secondaires pour le compte du propriétaire spécifié. Les mots de passe ne sont pas affichés.

```
vdmadmin –T –domainauth –list –owner domain\user
```

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 auprès d'Active Directory et de View.

- Des détails d'Active Directory sur le compte de l'utilisateur.
- L'appartenance à des groupes Active Directory.
- Les droits d'accès à la machine, notamment l'ID, le nom d'affichage, la description et le dossier de la machine, et si la machine a été désactivée.
- 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
```

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 distant. N'utilisez pas la commande pour administrer des postes de travail distants qui fonctionnent normalement.

Si un poste de travail distant 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 du système vCenter Server. Vous pouvez utiliser vCenter Client pour trouver le chemin d'inventaire d'une machine virtuelle pour un poste de travail distant 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 15-18 montre les options que vous pouvez spécifier pour déverrouiller ou verrouiller des machines virtuelles.

Tableau 15-18. 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
```

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 du Serveur de connexion View répliquées dans un groupe.

Syntaxe

```
vdmadmin –X [–b authentication_arguments] –collisions [–resolve]
```

Notes d'utilisation

Si des entrées LDAP en double sont créées dans au moins deux instances du Serveur de connexion View, 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 recherche cette condition d'erreur à intervalles réguliers, vous pouvez exécuter la commande `vdmadmin` sur l'une des instances du Serveur de connexion View du groupe pour détecter et résoudre manuellement les collisions d'entrées LDAP.

Options

Tableau 15-19 montre les options que vous pouvez spécifier pour détecter et résoudre les entrées LDAP en collision.

Tableau 15-19. 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 Serveur de connexion View.
`–resolve`	Résout toutes les collisions LDAP détectées.

Exemples

Détecter des collisions d'entrée LDAP dans un groupe Serveur de connexion View.

```
vdmadmin –X –collisions
```

Détecter et résoudre des collisions d'entrée LDAP.

```
vdmadmin –X –collisions –resolve
```

Index

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T