Administration d'Horizon Console

Décembre 2019
VMware Horizon 7 7.11

vmware®

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

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

Si vous avez des commentaires à propos de cette documentation, envoyez-les à l'adresse suivante :

docfeedback@vmware.com

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

VMware France SAS.
Tour Franklin
100-101 Terrasse Boieldieu
92042 Paris La Défense 8 Cedex
France
www.vmware.com/fr

Table des matières

Administration de VMware Horizon Console

1

Administration de VMware Horizon Console explique comment configurer et administrer VMware Horizon® 7, créer des administrateurs, configurer l'authentification utilisateur, configurer des stratégies et effectuer des tâches de gestion dans Horizon Console. Ce document explique également comment gérer et dépanner les composants de Horizon 7.

Pour obtenir plus d'informations sur l'utilisation d'Horizon Console pour configurer et gérer un environnement Architecture Cloud Pod, consultez le document *Administration d'Architecture Cloud Pod dans Horizon 7*.

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 centres de données et de la technologie des machines virtuelles.

Utilisation de VMware Horizon Console

2

VMware Horizon Console est la dernière version de l'interface Web avec laquelle vous pouvez créer et gérer des postes de travail virtuels, ainsi que des applications et des postes de travail publiés. La Horizon Console intègre également fonctionnalités de VMware Horizon Just-in-Time Management Platform (JMP) pour la gestion des espaces de travail.

La Horizon Console est disponible après l'installation et la configuration du Serveur de connexion Horizon.

Pour plus d'informations sur les fonctionnalités de JMP) Integrated Workflow, reportez-vous à la section Chapitre 10 Prise en main de JMP Integrated Workflow.

Ce chapitre contient les rubriques suivantes :

Fonctionnalités d'Horizon 7 prises en charge

Horizon Console est basé sur la technologie HTML5 et vous permet de gérer votre déploiement Horizon 7 complet. Horizon Console remplace Horizon Administrator basé sur Flash.

Pour plus d'informations sur les fonctionnalités d'Horizon 7 prises en charge avec Horizon Administrator, consultez le document *Administration d'Horizon 7*.

Les fonctionnalités suivantes sont prises en charge :

- Serveurs
  - Configuration du Serveur de connexion Horizon
  - Base de données des événements
- Autorisations
  - Droits d'utilisateur et de groupe
  - Droits de poste de travail

    - Droits d'application
    - Droits globaux
    - Stratégies générales
- Authentification
    - Authentification d'accès à distance
    - Accès non authentifié pour des applications publiées
    - Authentification par carte à puce
    - Administration déléguée basée sur des rôles
- Postes de travail virtuels
    - Pool à attribution dédiée automatisé de machines virtuelles complètes
    - Pools à attribution dédiée et flottante, automatisé, d'Instant Clone
    - Pools de postes de travail de clone lié automatisés
    - Pool à attribution flottante automatisé de machines virtuelles complètes
    - Pools de postes de travail manuels
    - Disques persistants
- Postes de travail publiés
    - Batteries de serveurs manuelles
    - Batteries de serveurs d'Instant Clone automatisées
    - Batteries de serveurs de clone lié automatisées
    - Pools de postes de travail RDS
- Applications publiées
    - Pools d'applications manuels
    - Pools d'applications à partir d'applications existantes
- Machines virtuelles
    - Machines virtuelles disponibles dans vCenter Server
    - Machines inscrites non disponibles dans vCenter Server
- Architecture Cloud Pod

Les fonctionnalités suivantes ne sont pas prises en charge :

- applications ThinApp
- Serveur de sécurité
- Serveur Mirage

Avantages de l'utilisation de la Horizon Console

Les avantages de l'utilisation de la Horizon Console incluent un processus plus facile de déploiement des postes de travail et des applications, une livraison de poste de travail juste-à-temps et une interface Web plus sécurisée réduit les risques de sécurité.

L'interface Web de la Horizon Console est mise à jour pour inclure des workflows faciles à utiliser pour le déploiement et le dépannage des postes de travail et des applications.

Horizon Console inclut également les fonctionnalités de JMP Integrated Workflow, qui comprennent les technologies d'Instant Clone, de VMware App Volumes et de VMware Dynamic Environment Manager dans un workflow intégré afin de fournir des postes de travail à la demande qui se déploient et sont mis à l'échelle rapidement. Pour plus d'informations, reportez-vous à la section À propos de JMP Integrated Workflow.

Horizon Console dispose d'une interface Web HTML5, qui est plus sécurisée et mise à jour afin d'éliminer les nombreux risques et vulnérabilités de sécurité.

Installation et configuration de la Horizon Console

L'URL de la Horizon Console est disponible dans l'interface Web d'Horizon Administrator une fois que vous avez utilisé le programme d'installation du Serveur de connexion Horizon pour installer et configurer le Serveur de connexion. JMP Integrated Workflow est disponible dans la Horizon Console une fois que vous avez utilisé le programme d'installation de JMP Server pour installer et configurer JMP Server.

Pour plus d'informations sur l'installation du Serveur de connexion, consultez le document *Installation d'Horizon 7*.

Pour plus d'informations sur l'installation et la configuration de JMPServer, reportez-vous au document *Guide d'installation et de configuration de VMware Horizon JMP Server*.

Se connecter à Horizon Console

Pour effectuer des tâches de déploiement de pool de postes de travail ou d'applications, des tâches de dépannage ou pour gérer des workflows JMP, vous devez vous connecter à la Horizon Console. Vous accédez à Horizon Console via une connexion sécurisée (TLS).

Conditions préalables

- Vérifiez que le Serveur de connexion Horizon est installé sur un ordinateur dédié.
- Un rôle prédéfini ou une combinaison de rôles prédéfinis pour se connecter à Horizon Console doit être attribué à un utilisateur. Vous ne pouvez pas vous connecter à Horizon Console lorsque l'utilisateur se voit attribuer un rôle personnalisé ou une combinaison de rôles prédéfinis et personnalisés. Pour plus d'informations sur la configuration de l'accès basé sur des rôles, reportez-vous à la section Configuration de l'administration déléguée basée sur des rôles.
- Vérifiez que vous utilisez un navigateur Web pris en charge par la Horizon Console. Pour plus d'informations sur les navigateurs Web pris en charge, consultez le document *Installation d'Horizon 7*.

Procédure

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

`https://server/admin`

Note Vous pouvez utiliser l'adresse IP si vous avez accès à une instance du Serveur de connexion lorsque le nom de l'hôte ne peut être résolu. Toutefois, l'hôte que vous contactez ne correspond pas au certificat TLS configuré pour l'instance du Serveur de connexion, ce qui bloque l'accès ou autorise l'accès avec une sécurité limitée.

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

Si vous ouvrez votre navigateur sur l'hôte du Serveur de connexion, 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 le Serveur de connexion.	Lorsque vous vous connectez pour la première fois, votre navigateur Web affiche la page **Bienvenue dans VMware Horizon 7**.
Le certificat auto-signé par défaut fourni avec le Serveur de connexion 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 TLS actuel.

2 Pour utiliser systématiquement la page de connexion Horizon Console, cliquez sur **Toujours utiliser cette option**.

Note Si vous cliquez sur **Toujours utiliser cette option** et que vous cliquez sur **Lancer**, la prochaine fois que vous ouvrez un onglet dans le navigateur Web et que vous entrez **`https://server/admin`**, vous obtenez toujours la page de connexion à Horizon Console. Pour accéder de nouveau à la page **Bienvenue dans VMware Horizon 7**, rendez-vous sur **`https://server/admin/#home`**.

3 Cliquez sur **Lancer** sous Horizon Console pour ouvrir la page de connexion à Horizon Console.

4 Ouvrez une session en tant qu'utilisateur actuel avec des informations d'identification pour accéder au compte Administrateurs.

Vous établissez une attribution initiale au rôle Administrateurs lorsque vous installez une instance autonome du Serveur de connexion ou la première instance du Serveur de connexion dans un groupe répliqué. Par défaut, le compte que vous utilisez pour installer le Serveur de connexion est sélectionné, mais vous pouvez modifier ce compte en groupe local Administrateurs ou en groupe global de domaine.

Si vous choisissez le groupe local Administrateurs, vous pouvez utiliser n'importe quel utilisateur de domaine ajouté à ce groupe directement ou via l'appartenance au groupe global. Vous ne pouvez pas utiliser des utilisateurs locaux ajoutés à ce groupe.

Étape suivante

Pour identifier l'espace de CPA ou le nom de cluster du Serveur de connexion que vous utilisez, vous pouvez afficher le nom dans l'en-tête Horizon Console et dans l'onglet Navigateur Web.

Configuration du Serveur de connexion Horizon dans Horizon Console

3

Après avoir installé et effectué la configuration initiale du Serveur de connexion Horizon, vous pouvez ajouter des instances de vCenter Server et des services Horizon Composer à votre déploiement Horizon 7, configurer des rôles pour déléguer des responsabilités d'administrateur et planifier des sauvegardes de vos données de configuration.

Ce chapitre contient les rubriques suivantes :

Configuration de vCenter Server et d'Horizon Composer dans Horizon Console

Pour utiliser des machines virtuelles en tant que postes de travail distants, vous devez configurer Horizon 7 pour communiquer avec vCenter Server. Pour créer et gérer des pools de postes de travail de clone lié, vous devez configurer des paramètres d'Horizon Composer dans Horizon Console.

Vous pouvez également configurer des paramètres de stockage pour Horizon 7. 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 Horizon Storage Accelerator pour vCenter Server.

Créer un compte d'utilisateur pour les opérations AD d'Horizon Composer

Si vous utilisez Horizon Composer, vous devez créer un compte d'utilisateur dans Active Directory qui permet à Horizon Composer d'effectuer certaines opérations dans Active Directory. Horizon Composer requiert que ce compte joigne les machines virtuelles de clone lié à votre domaine Active Directory.

Pour garantir la sécurité, créez un compte d'utilisateur séparé à utiliser avec Horizon 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 Horizon 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 du Serveur de connexion 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

   Note 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.

Étape suivante

Spécifiez le compte dans Horizon Console lorsque vous configurez des domaines Horizon Composer dans l'assistant **Ajouter une instance de vCenter Server** et lorsque vous configurez et déployez des pools de postes de travail de clone lié.

Installer la clé de licence produit dans Horizon Console

Avant de pouvoir utiliser le Serveur de connexion, vous devez entrer une clé de licence produit.

Note La clé de licence produit n'est pas requise si vous avez une licence d'abonnement Horizon 7. Pour plus d'informations sur les licences d'abonnement, reportez-vous à la section « Activation d'Horizon 7 pour les licences d'abonnement » dans le document *Installation d'Horizon 7*.

Lors de votre première ouverture de session, Horizon Console affiche la page Licence et utilisation.

Vous n'avez pas à configurer une clé de licence lorsque vous installez une instance du Serveur de connexion répliquée ou un serveur de sécurité. Les instances répliquées et les serveurs de sécurité utilisent la clé de licence commune stockée dans la configuration de View LDAP.

Note Le Serveur de connexion nécessite une clé de licence valide. La clé de licence de produit est une clé de 25 caractères.

Procédure

1. Dans Horizon Console, sélectionnez **Paramètres > Licence produit et utilisation**.
2. Dans le volet **Paramètres de licence**, cliquez sur **Modifier la licence**.
3. Saisissez le numéro de série de licence et cliquez sur **OK**.
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.

Ajouter des instances de vCenter Server à Horizon 7 dans Horizon Console

Vous devez configurer Horizon 7 pour qu'il se connecte aux instances de vCenter Server dans votre déploiement Horizon 7. vCenter Server crée et gère les machines virtuelles que Horizon 7 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 Horizon 7.

Horizon 7 se connecte à l'instance de vCenter Server via un canal sécurisé (TLS).

Conditions préalables

- Installez la clé de licence produit du Serveur de connexion.

- Configurez un utilisateur de vCenter Server autorisé à effectuer dans vCenter Server les opérations nécessaires à la prise en charge de Horizon 7. Pour utiliser Horizon Composer, vous devez accorder à l'utilisateur des privilèges supplémentaires.

  Pour plus d'informations sur la configuration d'un utilisateur de vCenter Server pour Horizon 7, consultez le document *Installation d'Horizon 7*.

- Vérifiez qu'un certificat de serveur TLS 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 Horizon 7.

- Vérifiez que toutes les instances du Serveur de connexion 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. 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 *Installation d'Horizon 7*.

- 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 Horizon 7.

- 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 Horizon 7 en mode FIPS, vérifiez que vous disposez de vCenter Server 6.0 ou version ultérieure et d'hôtes ESXi 6.0 ou version ultérieure.

  Pour plus d'informations, reportez-vous à la section « Installation d'Horizon 7 en mode FIPS » dans le document *Installation d'Horizon 7*.

- Familiarisez-vous avec les paramètres qui déterminent les limites d'opérations maximales pour vCenter Server et Horizon Composer.

Procédure

1. Dans Horizon Console, accédez à **Paramètres > Serveurs**.
2. Dans l'onglet **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.

   Note Si vous entrez un serveur à l'aide d'un nom DNS ou d'une URL, Horizon 7 n'effectue pas de recherche DNS pour vérifier si un administrateur a précédemment ajouté ce serveur à Horizon 7 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 (Facultatif) Sélectionnez **VMware Cloud on AWS** si vCenter Server est déployé sur VMware Cloud on AWS.

   Pour plus d'informations sur l'intégration d'Horizon 7 à VMware Cloud on AWS, consultez le document *Intégration d'Horizon 7*.

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

10 Cliquez sur **Suivant** et suivez les invites pour terminer l'assistant.

Étape suivante

Configurez les paramètres d'Horizon Composer.

- Si l'instance de vCenter Server est configurée avec un certificat TLS signé et si le Serveur de connexion approuve le certificat racine, l'assistant Ajouter une instance de vCenter Server affiche la page Paramètres d'Horizon 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 TLS par défaut.

Si Horizon 7 utilise plusieurs instances de vCenter Server, répétez cette procédure pour ajouter les autres instances de vCenter Server.

Configurer les paramètres d'Horizon Composer

Pour utiliser Horizon Composer, vous devez configurer les paramètres qui permettent à Horizon 7 de se connecter au service Horizon Composer. Horizon Composer peut être installé sur son propre hôte séparé ou sur le même hôte que vCenter Server.

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

Après le déploiement initial d'Horizon 7, vous pouvez migrer le service Horizon Composer vers un nouvel hôte pour prendre en charge un déploiement Horizon 7 en développement ou en évolution. Vous pouvez modifier les paramètres initiaux d'Horizon Composer dans Horizon Console, mais vous devez effectuer des étapes supplémentaires pour vous assurer que la migration réussit.

Conditions préalables

- 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 d'Horizon Composer.
- Vérifiez que vous avez configuré Horizon 7 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 Horizon 7 dans Horizon Console.
- Vérifiez que ce service Horizon Composer n'est pas déjà configuré pour se connecter à une instance de vCenter Server différente.

Procédure

1. Dans Horizon Console, accédez à **Paramètres > Serveurs**.
2. Dans l'onglet **vCenter Server**, cliquez sur **Ajouter**, puis renseignez les informations relatives à vCenter Server sur la page **Paramètres de vCenter Server** et cliquez sur **Suivant**.
3. Sur la page **Paramètres d'Horizon Composer**, si vous n'utilisez pas Horizon Composer, sélectionnez **Ne pas utiliser Horizon Composer**.

   Si vous sélectionnez **Ne pas utiliser Horizon Composer**, les autres paramètres d'Horizon Composer deviennent inactifs. Lorsque vous cliquez sur **Suivant**, l'assistant Ajouter une instance de vCenter Server affiche la page **Paramètres de stockage**.

4 Si vous utilisez Horizon Composer, sélectionnez l'emplacement de l'hôte Horizon Composer.

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

5 Cliquez sur **Suivant** pour afficher la page **Domaines Horizon Composer**.

Étape suivante

Configurez des domaines d'Horizon Composer.

- Si l'instance d'Horizon Composer est configurée avec un certificat TLS signé et si le Serveur de connexion approuve le certificat racine, l'assistant Ajouter une instance de vCenter Server affiche la page Domaines d'Horizon Composer.
- Si l'instance d'Horizon Composer est configurée avec un certificat par défaut, vous devez d'abord déterminer si vous acceptez l'empreinte numérique du certificat existant.

Configurer des domaines d'Horizon Composer

Vous devez configurer un domaine Active Directory dans lequel Horizon Composer déploie des postes de travail de clone lié. Vous pouvez configurer plusieurs domaines pour Horizon Composer. Après avoir ajouté vCenter Server et les paramètres d'Horizon Composer à Horizon 7, vous pouvez ajouter plus de domaines Horizon Composer en modifiant l'instance de vCenter Server dans Horizon Console.

Conditions préalables

- Votre administrateur Active Directory doit créer un utilisateur Horizon 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 d'Horizon Composer.
- Dans Horizon Console, vérifiez que vous avez rempli les pages **Paramètres de vCenter Server** et **Paramètres d'Horizon Composer** dans l'assistant **Ajouter une instance de vCenter Server**.

Procédure

1. Dans Horizon Console, accédez à **Paramètres > Serveurs**.
2. Sous l'onglet **vCenter Server**, cliquez sur **Ajouter**, puis renseignez les informations relatives à vCenter Server sur la page **Paramètres de vCenter Server** et cliquez sur **Suivant**.
3. Sur la page **Paramètres d'Horizon Composer**, si vous utilisez Horizon Composer, sélectionnez l'emplacement de l'hôte Horizon Composer et cliquez sur **Suivant**.

   Pour plus d'informations sur Horizon Composer, reportez-vous à la section Configurer les paramètres d'Horizon Composer.
4. Sur la page **Domaines Horizon Composer**, cliquez sur **Ajouter** pour ajouter l'utilisateur d'Horizon Composer aux informations du compte des opérations AD.
5. Saisissez le nom de domaine du domaine Active Directory.

   Par exemple : `domain.com`
6. Saisissez le nom d'utilisateur de domaine, notamment le nom de domaine, de l'utilisateur d'Horizon Composer.

   Par exemple : `domain.com\admin`
7. Saisissez le mot de passe du compte.
8. Cliquez sur **OK**.
9. 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.
10. Cliquez sur **Suivant** pour afficher la page **Paramètres de stockage**.

Étape suivante

Activez la récupération d'espace disque de machine virtuelle et configurez Horizon Storage Accelerator pour Horizon 7.

Ajouter un administrateur de domaine Instant Clone dans Horizon Console

Avant de créer un pool de postes de travail Instant Clone, vous devez ajouter un administrateur de domaine Instant Clone à Horizon 7.

Conditions préalables

- Vérifiez que l'administrateur de domaine Instant Clone dispose des privilèges de domaine Active Directory requis. Pour plus d'informations, consultez la section « Créer un compte d'utilisateur pour des opérations Instant Clone » dans le document *Installation d'Horizon 7*.

Procédure

1. Dans Horizon Console, sélectionnez **Paramètres > Comptes de domaine Instant Clone**.
2. Cliquez sur **Ajouter**.

3 Sélectionnez le domaine de l'administrateur de domaine Instant Clone.

4 Entrez le nom d'utilisateur et le mot de passe.

Étape suivante

Dans Horizon Console, vous pouvez ajouter ou supprimer un administrateur de domaine Instant Clone ou exporter la liste des administrateurs Instant Clone vers Microsoft Excel. Accédez à **Paramètres > Comptes de domaine Instant Clone** et sélectionnez un administrateur de domaine Instant Clone. Cliquez sur **Modifier** pour modifier le domaine et les informations de connexion de l'administrateur. Cliquez sur **Supprimer** pour supprimer un administrateur. Cliquez sur l'icône d'exportation pour exporter la liste des administrateurs Instant Clone vers un fichier Microsoft Excel.

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

Dans vSphere 5.1 ou versions ultérieures, vous pouvez activer la fonctionnalité de récupération d'espace disque pour Horizon 7. Horizon 7 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, Horizon 7 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 vSphere 5.1 ou versions ultérieures, lorsqu'une machine virtuelle parent est la version matérielle virtuelle 9 ou versions ultérieures, Horizon 7 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 Horizon Console 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.
- Elle n'affecte pas les disques persistants d'Horizon Composer.
- Elle fonctionne uniquement avec vSphere 5.1 ou versions ultérieures, et uniquement sur des machines disposant de la version matérielle virtuelle 9 ou versions ultérieures.
- 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.

Conditions préalables

- 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 Horizon Console, accédez à **Paramètres > Serveurs**.
2. Dans l'onglet **vCenter Server**, cliquez sur **Ajouter** et renseignez les pages de l'assistant **Ajouter une instance de vCenter Server** qui précèdent la page **Paramètres de stockage**.
3. Sur la page **Paramètres de stockage**, sélectionnez **Récupérer l'espace disque de machine virtuelle**.

   Cette option est sélectionnée par défaut si vous effectuez une nouvelle installation d'Horizon 7. Vous devez sélectionner **Récupérer l'espace disque de machine virtuelle** si vous effectuez une mise à niveau vers une version ultérieure d'Horizon 7.

Étape suivante

Sur la page **Paramètres de stockage**, configurez Horizon Storage Accelerator.

Pour terminer la configuration de la récupération d'espace disque dans Horizon 7, configurez la récupération d'espace pour les pools de postes de travail.

Configurer Horizon Storage Accelerator pour vCenter Server

Dans vSphere, vous pouvez configurer des hôtes ESXi afin de mettre en cache des données de disque de machine virtuelle. Cette fonction, appelée Horizon Storage Accelerator, utilise la fonction CBRC (Content Based Read Cache) dans les hôtes ESXi. Horizon Storage Accelerator améliore les performances d'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, Horizon 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 d'Horizon 7.

Vous activez la mise en cache sur vos hôtes ESXi en sélectionnant le paramètre Horizon Storage Accelerator dans l'assistant **Ajouter une instance de vCenter Server** dans Horizon Console, comme décrit dans cette procédure.

Assurez-vous que cette instance d'Horizon Storage Accelerator est également configurée pour des pools de postes de travail individuels. Pour fonctionner sur un pool de postes de travail, Horizon Storage Accelerator doit être activé pour vCenter Server et pour le pool de postes de travail individuel.

Horizon Storage Accelerator est activé pour les pools 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 Horizon 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 Horizon Storage Accelerator.

Horizon 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 d'Horizon 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 Horizon 7 qui partagent des hôtes ESXi, vous devez activer la fonction Horizon 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.

Conditions préalables

- Vérifiez que la version de vos hôtes vCenter Server et ESXi est la version 5.1 ou ultérieure.

  Dans un cluster ESXi, vérifiez que la version de tous les hôtes est la version 5.1 ou ultérieure.
- Vérifiez que l'utilisateur de vCenter Server a reçu le privilège **Hôte > Configuration > Paramètres avancés** dans vCenter Server.

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

Procédure

1. Dans Horizon Console, accédez à **Paramètres > Serveurs**.
2. Sous l'onglet **vCenter Server**, cliquez sur **Ajouter** et complétez les pages de l'assistant **Ajouter une instance de vCenter Server** qui précèdent la page **Paramètres de stockage**.
3. Sur la page **Paramètres de stockage**, sélectionnez **Activer Horizon Storage Accelerator**.

   Cette option est sélectionnée par défaut.
4. 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.
5. 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**.
6. Sur la page Paramètres de stockage, cliquez sur **Suivant**.
7. Après avoir vérifié les paramètres de la page **Prêt à terminer**, cliquez sur **Envoyer**.

Étape suivante

Configurez des paramètres pour les sessions et les connexions client. Reportez-vous à la section « Configuration des paramètres des sessions client » dans le document *Administration d'Horizon 7*.

Pour remplir les paramètres d'Horizon Storage Accelerator dans Horizon 7, configurez Horizon Storage Accelerator pour les pools de postes de travail. Reportez-vous à la section « Configurer Horizon Storage Accelerator pour des pools de postes de travail » dans le document *Configuration de postes de travail virtuels dans Horizon Console*.

Limites d'opérations simultanées pour vCenter Server et Horizon Composer

Lorsque vous ajoutez vCenter Server à Horizon 7 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 Horizon Composer.

Vous configurez ces options dans le panneau Paramètres avancés sur la page **Paramètres de vCenter Server** dans l'assistant **Ajouter une instance de vCenter Server**.

Tableau 3-1. Limites d'opérations simultanées pour vCenter Server et Horizon Composer

Paramètre	Description
Opérations d'approvisionnement de vCenter simultanées max.	Détermine le nombre maximal de demandes simultanées que le Serveur de connexion peut créer pour provisionner 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 le Serveur de connexion 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, reportez-vous à la section Définition d'un taux d'opérations d'alimentation simultanées pour prendre en charge les tempêtes d'ouverture de session des postes de travail distants Ce paramètre s'applique à des machines virtuelles complètes et à des clones liés.
Nombre maximal d'opérations de maintenance d'Horizon Composer simultanées	Détermine le nombre maximal d'opérations d'actualisation, de recomposition et de rééquilibrage Horizon Composer pouvant se dérouler simultanément sur des clones liés gérés par cette instance d'Horizon 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 maximal d'opérations d'approvisionnement d'Horizon 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 d'Horizon Composer. La valeur par défaut est 8. Ce paramètre ne s'applique qu'aux clones liés.
Nombre maximal d'opérations d'Instant Clone Engine simultanées	Détermine le nombre maximal d'opérations de création et de suppression pouvant se dérouler simultanément sur des Instant Clones gérés par cette instance de vCenter Server. Ce paramètre ne s'applique qu'aux Instant Clones.

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 Horizon 7*.

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 TLS par défaut

Lorsque vous ajoutez des instances de vCenter Server et d'Horizon Composer à Horizon 7, vous devez vérifier que les certificats TLS utilisés pour les instances de vCenter Server et d'Horizon Composer sont valides et approuvés par le Serveur de connexion. Si les certificats par défaut installés avec vCenter Server et Horizon 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 d'Horizon Composer est configurée avec un certificat signé par une autorité de certification, et si le certificat racine est approuvé par le Serveur de connexion, vous n'avez pas à accepter l'empreinte numérique 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 le Serveur de connexion 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.

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

Pour plus d'informations sur la configuration des certificats TLS, reportez-vous à la section « Configuration de certificats TLS pour des serveurs Horizon 7 Server » dans le document *Installation d'Horizon 7*.

Vous devez d'abord ajouter vCenter Server et Horizon Composer dans Horizon Console en utilisant l'assistant **Ajouter une instance de 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 vCenter Server.

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

Note Vous devez également accepter une empreinte de certificat lorsque vous mettez à niveau une version antérieure et lorsqu'un certificat de vCenter Server ou d'Horizon Composer n'est pas approuvé, ou si vous remplacez un certificat approuvé par un certificat non approuvé.

Procédure

1. Lorsqu'Horizon Console 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 d'Horizon Composer.
   a. Sur l'hôte de vCenter Server ou d'Horizon Composer, démarrez le composant logiciel enfichable MMC et ouvrez le magasin de certificats Windows.
   b. Accédez au certificat de vCenter Server ou d'Horizon 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 d'Horizon 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 Horizon Composer.

Supprimer une instance de vCenter Server d'Horizon 7

Vous pouvez supprimer la connexion entre Horizon 7 et une instance de vCenter Server. Lorsque vous le faites, Horizon 7 ne gère plus les machines virtuelles créées dans cette instance de vCenter Server.

Conditions préalables

Supprimez toutes les machines virtuelles associées à l'instance de vCenter Server. Pour plus d'informations sur la suppression de machines virtuelles, reportez-vous à la section relative à la suppression d'un pool de postes de travail dans le document *Configuration des postes de travail virtuels dans Horizon 7*.

Procédure

1 Dans Horizon Console, accédez à **Paramètres > Serveurs**.

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

3 Cliquez sur **Supprimer**.

Un message vous avertit qu'Horizon 7 n'a plus accès aux machines virtuelles gérées par cette instance de vCenter Server.

4 Cliquez sur **OK**.

Horizon 7 ne peut plus accéder aux machines virtuelles créées dans l'instance de vCenter Server.

Supprimer Horizon Composer d'Horizon 7

Vous pouvez supprimer la connexion entre Horizon 7 et le service Horizon Composer qui est associé à une instance de vCenter Server.

Avant de désactiver la connexion à Horizon Composer, vous devez supprimer d'Horizon 7 toutes les machines virtuelles de clone lié créées par Horizon Composer. Horizon 7 vous empêche de supprimer Horizon Composer si des clones liés associés existent toujours. Une fois que la connexion à Horizon Composer est désactivée, Horizon 7 ne peut plus provisionner ni gérer de nouveaux clones liés.

Procédure

1. Supprimez les pools de postes de travail de clone lié créés par Horizon Composer.
   a. Dans la Horizon Console, sélectionnez **Inventaire > 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 d'Horizon 7 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. En outre, les entrées de la base de données Horizon Composer associées et les réplicas créés par Horizon Composer sont supprimés.
   d. Répétez ces étapes pour chaque pool de postes de travail de clone lié créé par Horizon Composer.
2. Accédez à **Paramètres > Serveurs**.
3. Sous l'onglet **vCenter Servers**, sélectionnez l'instance de vCenter Server à laquelle Horizon Composer est associé.
4. Cliquez sur **Modifier**.
5. Sous l'onglet **Horizon Composer**, sous Paramètres d'Horizon Composer Server, sélectionnez **Ne pas utiliser Horizon Composer** et 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.

Étape suivante

Si vous avez l'intention d'installer Horizon Composer sur un autre hôte et de reconfigurer Horizon 7 pour se connecter au nouveau service Horizon Composer, vous devez effectuer des étapes supplémentaires. Pour plus d'informations sur la migration d'Horizon Composer sans machines virtuelles de clone lié, consultez le document *Administration d'Horizon 7*.

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 Horizon 7, 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 Horizon dans Horizon Console

Après avoir terminé la configuration initiale du Serveur de connexion Horizon, vous devez planifier des sauvegardes régulières de vos données de configuration d'Horizon 7 et d'Horizon Composer.

Pour plus d'informations sur la sauvegarde et la restauration de votre configuration de Horizon 7, reportez-vous à Sauvegarde des données du Serveur de connexion Horizon et d'Horizon Composer.

Configuration des paramètres des sessions client dans Horizon Console

Vous pouvez configurer des paramètres généraux qui affectent les sessions et connexions client gérées par une instance du Serveur de connexion 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.

Paramètres généraux pour des sessions client dans Horizon Console

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 Horizon Console, si des messages de préouverture de session et d'avertissement sont affichés, si Horizon Console traite Windows Server comme un système d'exploitation pris en charge pour les postes de travail distants, ainsi que d'autres paramètres.

Dans Horizon Console, vous pouvez configurer des paramètres généraux en accédant à **Paramètres > Paramètres généraux > Paramètres généraux**.

Les modifications apportées à tout paramètre du tableau suivant prennent effet immédiatement. Vous n'avez pas à redémarrer Serveur de connexion Horizon 7 ou Horizon Client.

Tableau 3-2. Paramètres généraux pour des sessions client

Paramètre	Description
Délai d'expiration de la session de View Administrator	Détermine la durée pendant laquelle une session Horizon Console inactive continue avant d'expirer. **Important** Définir le délai d'expiration de la session Horizon Console sur un nombre de minutes élevé augmente le risque d'utilisation non autorisée de Horizon Console. Soyez prudent lorsque vous autorisez une session inactive à durer longtemps. Par défaut, le délai d'expiration de la session Horizon Console est de 30 minutes. Vous pouvez définir un délai d'expiration de session compris entre 10 et 4 320 minutes (72 heures). Avant qu'une session n'expire, un message d'avertissement s'affiche avec un compte à rebours de 60 secondes. Si vous cliquez dans la session avant la fin du compte à rebours, la session se poursuit. Après 60 secondes, un message d'erreur s'affiche pour vous informer que la session a expiré et que vous devez vous reconnecter.
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 Horizon 7. 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, Horizon 7 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. **Note** 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 Horizon 7 Agent 6.0 ou version ultérieure ou Horizon Agent 7.0 ou version ultérieure, le Serveur de connexion Horizon 7 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 Horizon 7 ou quitter Horizon Client, et se reconnecter au Serveur de connexion Horizon 7. Cependant, si le poste de travail est lancé à partir de Workspace ONE ou VMware Identity Manager et s'il est verrouillé, les informations d'identification d'authentification unique ne sont pas supprimées.
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 Horizon Console après quelques minutes. La page Tableau de bord de Horizon Console est également mise à jour après quelques minutes. Par défaut, ce paramètre n'est pas activé.

Tableau 3-2. 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**, Horizon 7, 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**, Horizon 7 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 Horizon 7, quelle que soit son activité sur le périphérique client. Si cette option est définie sur **Jamais**, Horizon 7 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**.
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 3-2. 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, Horizon Console affiche toutes les machines Windows Server disponibles, y compris celles sur lesquelles des composants de serveur Horizon 7 sont installés. **Note** Le logiciel Horizon Agent ne peut pas coexister sur la même machine virtuelle ou physique avec tout autre composant logiciel du serveur Horizon 7, notamment un serveur de sécurité, un Serveur de connexion Horizon 7 ou Horizon 7 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, Horizon 7 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. **Note** Cette fonctionnalité est disponible dans Horizon 7 version 7.0.2 et ultérieures.
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.

Tableau 3-2. Paramètres généraux pour des sessions client (suite)

Paramètre	Description
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 le paramètre **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 empêche les utilisateurs d'entrer des informations de domaine dans la zone de texte Nom d'utilisateur, et la connexion échoue toujours. Cela ne s'applique pas à Horizon Client 5.0 et aux versions ultérieures s'il existe un domaine d'utilisateur unique. **Important** Pour plus d'informations sur la sécurité et la facilité d'utilisation de ce paramètre, consultez le document *Sécurité d'Horizon 7*.
Envoyer la liste de domaines	Cochez la case pour permettre au Serveur de connexion d'envoyer la liste des noms de domaine au client avant l'authentification de l'utilisateur. **Important** Pour plus d'informations sur la sécurité et la facilité d'utilisation de ce paramètre, consultez le document *Sécurité d'Horizon 7*.

Paramètres généraux de sécurité des sessions et connexions client dans Horizon Console

Les paramètres généraux de sécurité déterminent si les clients sont authentifiés à nouveau après des interruptions, si le mode de sécurité des messages est activé et si l'état de sécurité est amélioré.

Dans Horizon Console, vous pouvez configurer des paramètres de sécurité généraux en accédant à **Paramètres > Paramètres généraux > Paramètres de sécurité**.

TLS est requis pour toutes les connexions d'Horizon Client et d'Horizon Console à Horizon 7. Si votre déploiement d'Horizon 7 utilise des équilibrages de charge ou d'autres serveurs intermédiaires clients, vous pouvez décharger TLS sur eux et configurer des connexions non-TLS sur des instances du Serveur de connexion et des serveurs de sécurité individuels.

Tableau 3-3. 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 Horizon 7 sont signés et vérifiés. ■ Lorsque le mode est défini sur **Amélioré**, la sécurité est fournie par TLS à authentification mutuelle. Connexions JMS et contrôle d'accès sur les rubriques JMS. 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 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 Horizon 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**.

Paramètres généraux de restriction du client pour les sessions client dans Horizon Console

Les paramètres généraux de restriction du client peuvent limiter le lancement de postes de travail virtuels, de postes de travail publiés et d'applications publiées à des clients et des versions spécifiques.

Dans Horizon Console, vous pouvez configurer les paramètres généraux de restriction du client en accédant à **Paramètres > Paramètres généraux > Paramètres de restriction du client** et en entrant la version d'Horizon Client.

La version d'Horizon Client doit être 4.5.0 ou ultérieure, sauf Horizon Client pour Chrome, qui doit être 4.8.0 ou version ultérieure. Les versions antérieures d'Horizon Client ne sont pas autorisées à se connecter à des postes de travail distants et à des applications publiées lorsque cette fonctionnalité est configurée.

Note Les paramètres de restriction du client empêchent uniquement les utilisateurs finaux de lancer des applications publiées et des postes de travail distants. Cette fonctionnalité n'empêche pas les utilisateurs finaux de se connecter à Horizon 7.

Tableau 3-4. Paramètres généraux de restriction du client pour les sessions client

Paramètre	Description
Horizon Client pour Windows	Entrez un numéro de version de Horizon Client qui correspond à 4.5.0 ou version ultérieure.
Horizon Client pour Linux	Entrez un numéro de version de Horizon Client qui correspond à 4.5.0 ou version ultérieure.
Horizon Client pour Mac	Entrez un numéro de version de Horizon Client qui correspond à 4.5.0 ou version ultérieure.
Horizon Client pour iOS	Entrez un numéro de version de Horizon Client qui correspond à 4.5.0 ou version ultérieure.
Horizon Client pour Android	Entrez un numéro de version de Horizon Client qui correspond à 4.5.0 ou version ultérieure.
Horizon Client pour UWP	Entrez un numéro de version de Horizon Client qui correspond à 4.5.0 ou version ultérieure.
Horizon Client pour Chrome	Entrez un numéro de version de Horizon Client qui correspond à 4.8.0 ou version ultérieure.
Horizon Client pour HTML Access	Entrez un numéro de version de Horizon Client qui correspond à 4.5.0 ou version ultérieure.
Bloquer les clients supplémentaires	Lorsque vous sélectionnez cette option, tous les autres types de clients, à l'exception des clients Horizon hérités, ne peuvent pas lancer des postes de travail ou des applications publiées. Cependant, si vous souhaitez que les utilisateurs finaux utilisent d'autres types de clients pour lancer des postes de travail et des applications publiées, vous devez ajouter le type de client à l'attribut `pae-AdditionalClientTypes` LDAP pour contourner les paramètres de blocage pour ce type de client. Vous pouvez utiliser l'utilitaire ADSI Edit pour modifier les attributs LDAP sur le Serveur de connexion. Dans l'utilitaire ADSI Edit, l'attribut `pae-AdditionalClientTypes` LDAP est disponible sous `CN=Common`, `OU=Global`, `OU=Properties`, `DC=vdi`, `DC=vmware`, `DC=int`.
Message	Entrez le message à afficher si un utilisateur tente de lancer un poste de travail ou une application publiée à partir d'un type ou d'une version de client ne figurant pas dans la liste blanche.

Désactiver ou activer le Serveur de connexion Horizon dans Horizon Console

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

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

Votre déploiement de Horizon 7 détermine comment les utilisateurs sont affectés en désactivant une instance.

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

Procédure

1. Dans Horizon Console, sélectionnez **Paramètres > Serveurs**.
2. Dans l'onglet **Serveurs de connexion**, sélectionnez l'instance du Serveur de connexion.
3. Cliquez sur **Désactiver**.

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

Modifier les URL externes des instances du Serveur de connexion Horizon

Vous pouvez utiliser Horizon Console pour modifier les URL externes des instances du Serveur de connexion.

Par défaut, un hôte du Serveur de connexion 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.

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. 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. 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.

Procédure

1. Dans Horizon Console, sélectionnez **Paramètres > Serveurs**.
2. Dans l'onglet **Serveurs de connexion**, sélectionnez l'instance du Serveur de connexion et cliquez sur **Modifier**.
3. 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://horizon.example.com:443

   Note Vous pouvez utiliser l'adresse IP si vous avez accès à une instance du Serveur de connexion lorsque le nom de l'hôte ne peut être résolu. Toutefois, dans ce cas, l'hôte que vous contactez ne correspond pas au certificat TLS configuré pour l'instance du Serveur de connexion, ce qui bloque l'accès ou autorise l'accès avec une sécurité limitée.
4. 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 du Serveur de connexion.
5. 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.
6. Vérifiez que toutes les adresses de cette boîte de dialogue permettent aux systèmes clients d'atteindre cet hôte.
7. Cliquez sur **OK** pour enregistrer vos modifications.

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

Enregistrer des passerelles dans Horizon Console

Les instances d'Horizon Client se connectent via une passerelle ou un dispositif Unified Access Gateway que vous enregistrez dans Horizon Console.

Vous pouvez enregistrer ou annuler l'enregistrement des passerelles dans Horizon Console. Pour annuler l'enregistrement de la passerelle, sélectionnez la passerelle ou un dispositif Unified Access Gateway et cliquez sur **Annuler l'enregistrement**.

Procédure

1. Dans Horizon Console, sélectionnez **Paramètres > Serveurs**.
2. Dans l'onglet **Passerelles**, cliquez sur **Enregistrer**.
3. Entrez le nom de domaine complet de la passerelle ou du dispositif Unified Access Gateway.
4. Cliquez sur **OK**.

Configuration de l'authentification par carte à puce

4

Pour une sécurité accrue, vous pouvez configurer une instance du Serveur de connexion 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 d'Horizon 7*. 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://docs.vmware.com/fr/VMware-Horizon-Client/index.html.

Ce chapitre contient 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 ou à un serveur de sécurité configuré pour l'authentification par carte à puce, l'instance du Serveur de connexion 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 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 Horizon Console. 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 Unified Access Gateway pour sécuriser l'accès externe, vous devez configurer le dispositif Unified Access Gateway pour qu'il prenne en charge la fonctionnalité d'aide-mémoire du nom d'utilisateur de carte à puce. La fonctionnalité d'aide-mémoire du nom d'utilisateur de carte à puce n'est prise en charge qu'avec Unified Access Gateway 2.7.2 et versions ultérieures. Pour plus d'informations sur l'activation de la fonctionnalité d'aide-mémoire du nom d'utilisateur de carte à puce dans un dispositif Unified Access Gateway, consultez le document *Déploiement et configuration d'Unified Access Gateway*.

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 Horizon

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 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

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

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

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 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 Horizon

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

5 Configurer les paramètres de carte à puce dans Horizon Console

Vous pouvez utiliser Horizon Console 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.

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.

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.

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 et les serveurs de sécurité utilisent ces informations pour authentifier les utilisateurs et les administrateurs de cartes à puce.

Conditions préalables

- 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 et Obtenir le certificat d'une autorité de certification de Windows.

  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 ou du serveur de sécurité. Consultez le document *Installation d'Horizon 7* pour plus d'informations.

Procédure

1. Sur votre hôte du Serveur de connexion 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.

   Note 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 ou l'hôte du serveur de sécurité.

   Par exemple : *`install_directory`*`\VMware\VMware View\Server\sslgateway\conf\`*`truststorefile.key`*

Étape suivante

Modifiez des propriétés de configuration du Serveur de connexion pour activer l'authentification par carte à puce.

Modifier des propriétés de configuration du Serveur de connexion Horizon

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

Conditions préalables

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 TLS/SSL sur l'hôte du Serveur de connexion.

   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 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
```

Étape suivante

Si vous avez configuré l'authentification par carte à puce pour une instance du Serveur de connexion, configurez les paramètres d'authentification par carte à puce dans Horizon Console.

Configurer les paramètres de carte à puce dans Horizon Console

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

Conditions préalables

- Modifiez les propriétés de configuration du Serveur de connexion sur votre hôte du Serveur de connexion.
- Vérifiez qu'Horizon Client établit des connexions HTTPS directement à votre hôte du Serveur de connexion ou du serveur de sécurité. L'authentification par carte à puce n'est pas prise en charge si vous déchargez TLS sur un périphérique intermédiaire.

Procédure

1. Dans Horizon Console, sélectionnez **Paramètres > Serveurs**.
2. Dans l'onglet **Serveurs de connexion**, sélectionnez l'instance du Serveur de connexion 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 Sous l'onglet **Authentification**, sélectionnez une option de configuration dans le menu déroulant **Authentification par carte à puce des utilisateurs** de la section Authentification Horizon.

Option	Action
Non autorisée	L'authentification par carte à puce est désactivée sur l'instance du Serveur de connexion.
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. 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. 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. Ces utilisateurs doivent s'authentifier à nouveau avec leur carte à puce et leur code PIN lorsqu'ils se connectent au Serveur de connexion. **Note** 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 stratégie 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 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 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 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 des administrateurs se connectant à Horizon Console, sélectionnez une option de configuration dans le menu déroulant **Authentification par carte à puce des administrateurs** dans la section **Authentification Horizon Administrator**.

Option	Action
Non autorisée	L'authentification par carte à puce est désactivée sur l'instance du Serveur de connexion.
Facultative	Les administrateurs peuvent utiliser l'authentification par carte à puce ou l'authentification par mot de passe pour se connecter à Horizon Console. 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 Horizon Console.

5 Cliquez sur **OK**.

6 Redémarrez le service Serveur de connexion.

Vous devez redémarrer le service Serveur de connexion 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.

Les utilisateurs et les administrateurs actuellement connectés ne sont pas affectés par les modifications des paramètres de carte à puce.

Étape suivante

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.

Vérifiez votre configuration d'authentification par carte à puce. Reportez-vous à la section Vérifier votre configuration de l'authentification par carte à puce dans Horizon Console.

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 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 Horizon Console.

Pour plus d'informations sur la configuration de l'authentification par carte à puce sur Unified Access Gateway, consultez la documentation Unified Access Gateway.

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 Horizon Console.
2. Allongez la période d'expiration des métadonnées du Serveur de connexion 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.
3. Si nécessaire, configurez le périphérique tiers afin d'utiliser les métadonnées de fournisseur de service du Serveur de connexion.

   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

  Comme les ouvertures de session par carte à puce reposent sur des noms d'utilisateur principaux (UPN), les comptes Active Directory d'utilisateurs et d'administrateurs qui utilisent des cartes à puce pour s'authentifier dans Horizon 7 doivent avoir un UPN valide.

- 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.

- 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.

- 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.

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 Active Directory d'utilisateurs et d'administrateurs qui utilisent des cartes à puce pour s'authentifier dans Horizon 7 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.

Note 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.

Conditions préalables

- 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**.

Version d'AD	Chemin de navigation
Windows 2012 R2	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**.
Windows 2016	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.

Étape suivante

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.

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**.
Windows 2012 R2	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**.
Windows 2016	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 dans Horizon Console

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 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, vérifiez le paramètre d'authentification par carte à puce dans Horizon Console.

  a Sélectionnez **Paramètres > Serveurs**.

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

Horizon 7 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 ou sur un serveur de sécurité. Lorsqu'une instance du Serveur de connexion 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 ou du serveur de sécurité.

Vous pouvez configurer la CRL et OCSP sur la même instance du Serveur de connexion ou sur le même serveur de sécurité. Lorsque vous configurez les deux types de vérification de la révocation des certificats, Horizon 7 tente d'utiliser d'abord OCSP et revient à la CRL si OCSP échoue. Horizon 7 ne revient pas à OCSP si la CRL échoue.

- 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, Horizon 7 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

  Lorsque vous configurez la vérification de la révocation des certificats OCSP, Horizon 7 envoie une demande à un répondeur OCSP pour déterminer l'état de révocation d'un certificat utilisateur spécifique. Horizon 7 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

  Lorsque vous configurez la vérification de la liste de révocation de certificats, Horizon 7 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

  Lorsque vous configurez la vérification de la révocation des certificats OCSP, Horizon 7 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

  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, Horizon 7 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 Horizon 7 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, Horizon 7 envoie une demande à un répondeur OCSP pour déterminer l'état de révocation d'un certificat utilisateur spécifique. Horizon 7 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.

Horizon 7 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, Horizon 7 lit une liste de révocation de certificats pour déterminer l'état de révocation d'un certificat utilisateur de carte à puce.

Conditions préalables

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.

Procédure

1. Créez ou modifiez le fichier `locked.properties` dans le dossier de configuration de la passerelle TLS/SSL sur l'hôte du Serveur de connexion 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 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, Horizon 7 envoie une demande de vérification à un répondeur OCSP pour déterminer l'état de révocation d'un certificat de carte à puce.

Conditions préalables

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.

Procédure

1. Créez ou modifiez le fichier `locked.properties` dans le dossier de configuration de la passerelle TLS/SSL sur l'hôte du Serveur de connexion 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 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 4-1. Propriétés de la vérification de la révocation des certificats de carte à puce répertorie les propriétés du fichier `locked.properties` concernant la vérification de la révocation des certificats.

Tableau 4-1. 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, Horizon 7 utilise la liste de révocation de certificats sur le certificat utilisateur si `allowCertCRLs` est défini sur **`true`** ou n'est pas spécifié. Si Horizon 7 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`**, Horizon 7 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. Horizon 7 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`**, Horizon 7 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

5

Horizon 7 utilise votre infrastructure Active Directory existante pour l'authentification et la gestion des utilisateurs et des administrateurs. Vous pouvez également intégrer Horizon 7 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 contient les rubriques suivantes :

Utilisation de l’authentification à deux facteurs

Vous pouvez configurer une instance du Serveur de connexion Horizon pour forcer les utilisateurs à 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.
- Horizon 7 fournit également une interface d'extension standard ouverte pour permettre aux fournisseurs de solutions tiers d'intégrer des extensions d'authentification avancées dans Horizon 7.

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 configurer ces serveurs et les rendre accessibles à l’hôte du Serveur de connexion . 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 disposez de plusieurs instances du Serveur de connexion , 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 à distance depuis l'extérieur du réseau d'entreprise, sur Internet.

Horizon 7 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 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.
- Activer l'authentification à deux facteurs dans Horizon Console

  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 dans Horizon Console.
- Résolution du refus d'accès RSA SecureID

  L'accès est refusé lorsqu'Horizon Client se connecte avec l'authentification RSA SecurID.
- Résolution du refus d'accès RADIUS

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

Ouvrir une session avec l'authentification à deux facteurs

Lorsqu'un utilisateur se connecte à une instance du Serveur de connexion 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 Horizon 7, 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 Horizon Console

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 dans Horizon Console.

Conditions préalables

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 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 entrez ces valeurs dans Horizon Console. Vous pouvez entrer des valeurs pour un authentificateur RADIUS principal et secondaire.

Procédure

1. Dans Horizon Console, accédez à **Paramètres > Serveurs**.
2. Dans l'onglet **Serveurs de connexion**, sélectionnez l'instance du Serveur de connexion et cliquez sur **Modifier**.
3. Sous l'onglet **Authentification**, dans le menu déroulant **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 le menu déroulant **Authentificateur**, sélectionnez **Créer un authentificateur** et renseignez la page.

- Pour activer les libellés de nom d'utilisateur et de code secret personnalisés qui s'affichent dans la boîte de dialogue d'authentification RADIUS pour les utilisateurs finaux, entrez des libellés personnalisés dans les champs **Étiquette du nom d'utilisateur** et **Étiquette du code secret**.
- 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 sont 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. 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, 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.

Étape suivante

Si vous disposez d'un groupe répliqué d'instances du Serveur de connexion 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 SecureID

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 Horizon Console, accédez à **Paramètres > Serveurs**.
2. Dans l'onglet **Serveurs de connexion**, sélectionnez l'instance du Serveur de connexion et cliquez sur **Modifier**.
3. Dans l'onglet **Authentification**, dans le menu déroulant **Authentification à deux facteurs** de la section **Authentification avancée**, sélectionnez **RSA SecureID**.
4. Sélectionnez **Effacer le code secret du nœud** et cliquez sur **OK**.
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 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 Horizon 7.

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 en tant que client RADIUS. Chaque instance du Serveur de connexion 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 du secret partagé de l'instance du Serveur de connexion 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 Horizon 7 à VMware Workspace ONE, VMware Identity Manager, ou une passerelle ou un équilibrage de charge tiers complet. Lorsque vous configurez SAML pour un périphérique tiers, reportez-vous à la documentation du fournisseur pour plus d'informations sur la configuration de Horizon 7 afin qu'il interagisse avec lui. 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 ONE, VMware Identity Manager ou un périphérique tiers, vous devez créer un authentificateur SAML dans Horizon 7. Un authentificateur SAML contient l'approbation et l'échange de métadonnées entre Horizon 7 et Workspace ONE, VMware Identity Manager ou le périphérique tiers. Vous associez un authentificateur SAML à une instance du Serveur de connexion.

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

L'intégration entre Horizon 7 et VMware Identity Manager (anciennement nommée Workspace ONE) utilise la norme SAML 2.0 pour établir une approbation mutuelle, qui est essentielle pour la fonctionnalité de Single Sign-On (SSO). Lorsque l'authentification unique est activée, les utilisateurs qui se connectent à VMware Identity Manager ou Workspace ONE 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 Horizon 7 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 où se trouve 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 l'envoie à l'instance du Serveur de connexion. L'instance du Serveur de connexion utilise l'artefact SAML pour récupérer l'assertion SAML depuis VMware Identity Manager.

Lorsqu'une instance du Serveur de connexion reçoit une assertion SAML, elle la valide, 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 Horizon 7 implique la configuration de VMware Identity Manager avec les informations de Horizon 7 et la configuration de Horizon 7 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 Horizon 7. Un authentificateur SAML assure l'échange d'approbations et de métadonnées entre Horizon 7 et VMware Identity Manager. Vous associez un authentificateur SAML à une instance du Serveur de connexion.

Note 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 Horizon Console. 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 Horizon 7 et vous ne pourrez pas configurer le pool dans VMware Identity Manager.

Configurer un authentificateur SAML dans Horizon Console

Pour lancer des applications et des postes de travail à distance depuis VMware Identity Manager ou vous connecter à des applications et des postes de travail à distance via une passerelle ou un équilibreur de charge tiers, vous devez créer un authentificateur SAML dans Horizon Console. Un authentificateur SAML contient l'approbation et l'échange de métadonnées entre Horizon 7 et le périphérique auquel se connectent les clients.

Vous associez un authentificateur SAML à une instance du Serveur de connexion. Si votre déploiement inclut plusieurs instances du Serveur de connexion, 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 (Statique) Unified Access Gateway et les maintenir actifs. Vous pouvez établir des connexions via l'un de ces authentificateurs.

Vous pouvez configurer plusieurs authentificateurs SAML sur un Serveur de connexion, 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 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 Unified Access Gateway de VMware, consultez la documentation Unified Access Gateway.

Conditions préalables

- Vérifiez qu'Workspace ONE, 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 du 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 d'Horizon 7*.
- Notez le nom de domaine complet ou l'adresse IP du serveur Workspace ONE, du serveur VMware Identity Manager ou de l'équilibrage de charge externe.
- Si vous utilisez Workspace ONE ou VMware Identity Manager, notez l'URL de l'interface Web du connecteur.
- Si vous créez un authentificateur pour un dispositif Unified Access Gateway 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 Horizon Console, accédez à **Paramètres > 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 dans votre déploiement pour disposer de paramètres d'authentification SAML différents, adaptés à vos besoins.

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 un dispositif Unified Access Gateway 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 un dispositif Unified Access Gateway 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. 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 un dispositif Unified Access Gateway ou 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 Horizon 7 et VMware Identity Manager ou le périphérique tiers.

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

Étape suivante

Allongez la période d'expiration des métadonnées du Serveur de connexion 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.

Configurer le support de proxy pour VMware Identity Manager

Horizon 7 fournit un support de proxy pour le serveur VMware Identity Manager (vIDM). Les détails de proxy, tels que le nom d'hôte et le numéro de port, peuvent être définis dans la base de données ADAM, et les demandes HTTP sont acheminées via le proxy.

Cette fonctionnalité prend en charge un déploiement hybride dans le cadre duquel le déploiement de Horizon 7 sur site peut communiquer avec un serveur vIDM qui est hébergé dans le cloud.

Conditions préalables

Procédure

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

2 Développez l'arborescence d'ADAM ADSI sous le chemin d'objet : `cd=vdi,dc=vmware,dc=int,ou=Properties,ou=Global,cn=Common Attributes`.

3 Sélectionnez **Action > Propriétés** et ajoutez les valeurs des entrées **`pae-SAMLProxyName`** et **`pae-SAMLProxyPort`**.

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

Si vous ne modifiez pas la période d'expiration, le Serveur de connexion cesse d'accepter les assertions SAML de l'authentificateur SAML, tel qu'un dispositif Unified Access Gateway 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 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 génère des métadonnées avec une période d'expiration de 90 jours.

Conditions préalables

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.
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, 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 qui doit s'écouler avant qu'un Serveur de connexion à distance 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 puisse être utilisé comme fournisseur de service

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

Conditions préalables

Vérifiez que vous avez créé un authentificateur SAML pour le fournisseur d'identité : Unified Access Gateway ou une passerelle ou un équilibrage de charge tiers.

Procédure

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

   `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.

Cette page affiche les métadonnées SAML du Serveur de connexion.

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" ...
```

Étape suivante

Utilisez la procédure appropriée sur le fournisseur d'identité pour copier les métadonnées SAML du Serveur de connexion. Consultez la documentation d'Unified Access Gateway 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 comme authentification facultative ou obligatoire sur une instance du Serveur de connexion et que vous associez plusieurs authentificateurs SAML dynamiques à cette instance, le temps de réponse pour lancer des postes de travail à distance à partir des autres authentificateurs SAML dynamiques augmente si des authentificateurs SAML dynamiques deviennent inaccessibles.

Vous pouvez réduire le temps de réponse du lancement des postes de travail à distance sur les autres authentificateurs SAML dynamiques en utilisant Horizon Console pour désactiver les authentificateurs SAML dynamiques inaccessibles. Pour plus d'informations sur la désactivation d'un authentificateur SAML, reportez-vous à la section Configurer un authentificateur SAML dans Horizon Console.

Configurer des stratégies d'accès Workspace ONE dans Horizon Console

Les administrateurs Workspace ONE ou VMware Identity Manager (vIDM) peuvent configurer des stratégies d'accès pour restreindre l'accès aux applications et postes de travail autorisés dans Horizon 7. Pour appliquer des stratégies créées dans vIDM, faites passer Horizon Client en mode Workspace ONE afin qu'il puisse transférer l'utilisateur dans le client Workspace ONE pour lancer des autorisations. Lorsque vous vous connectez à Horizon Client, la stratégie d'accès vous amène à vous connecter via Workspace ONE pour accéder à vos applications et postes de travail publiés.

Conditions préalables

- Configurez des stratégies d'accès pour les applications dans Workspace ONE. Pour plus d'informations sur la définition de stratégies d'accès, reportez-vous au document *Guide d'administration de VMware Identity Manager*.
- Autorisez les utilisateurs à accéder aux applications et postes de travail publiés dans Horizon Console.

Procédure

1. Dans Horizon Console, accédez à **Paramètres > Serveurs**.
2. Dans l'onglet **Serveurs de connexion**, sélectionnez une instance de serveur associée à l'authentificateur SAML et cliquez sur **Modifier**.
3. Dans l'onglet **Authentification**, définissez l'option **Délégation de l'authentification à VMware Horizon (authentificateur SAML 2.0)** sur **Requise**.

   L'option Requis active l'authentification SAML. L'utilisateur final peut se connecter au serveur Horizon Server uniquement avec un jeton SAML fourni par vIDM ou un fournisseur d'identité tiers. Vous ne pouvez pas démarrer manuellement des postes de travail ou des applications à partir d'Horizon Client.
4. Sélectionnez **Activer le mode Workspace ONE**.
5. Dans la zone de texte **Nom d'hôte du serveur Workspace ONE**, entrez le nom de domaine complet du nom d'hôte Workspace ONE.
6. (Facultatif) Sélectionnez **Bloquer les connexions des clients ne prenant pas en charge le mode Workspace ONE** pour empêcher les clients Horizon Client qui prennent en charge le mode Workspace ONE d'accéder aux applications.

   Les clients Horizon Client antérieurs à la version 4.5 ne prennent pas en charge le mode Workspace ONE. Si vous sélectionnez cette option, les clients Horizon Client antérieurs à la version 4.5 ne peuvent pas accéder aux applications dans Workspace ONE. Le mode Workspace ONE n'est pas activé pour les versions postérieures à la version 7.2 d'Horizon 7 si la version Workspace ONE est antérieure à la version 2.9.1.

Configurer l'authentification biométrique

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

Conditions préalables

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.
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, 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 ou le périphérique client.

Authentification d'utilisateurs et de groupes

6

Une fois que vous êtes connecté à Horizon Console, vous pouvez configurer l'authentification des utilisateurs et des groupes pour contrôler l'accès aux applications et aux postes de travail.

Vous pouvez configurer l'accès à distance pour empêcher les utilisateurs et les groupes d'accéder à des postes de travail depuis l'extérieur du réseau. Vous pouvez 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.

Ce chapitre contient les rubriques suivantes :

Limiter l'accès à des postes de travail distants en dehors du réseau

Vous pouvez autoriser l'accès à des utilisateurs et des groupes autorisés spécifiques depuis un réseau externe tout en limitant l'accès à d'autres utilisateurs et groupes autorisés. Tous les utilisateurs autorisés auront accès à des postes de travail et des applications dans le réseau interne. Si vous choisissez de ne pas limiter l'accès à des utilisateurs spécifiques depuis le réseau externe, tous les utilisateurs autorisés auront accès depuis le réseau externe.

Pour des raisons de sécurité, les administrateurs peuvent avoir besoin d'empêcher des utilisateurs et des groupes en dehors du réseau d'accéder à des applications et des postes de travail distants sur le réseau. Lorsqu'un utilisateur restreint accède au système depuis un réseau externe, un message indiquant que l'utilisateur n'est pas autorisé à utiliser le système s'affiche. L'utilisateur doit se trouver dans le réseau interne pour obtenir l'accès à des droits de pool de postes de travail et d'applications.

Configurer l'accès distant

Vous pouvez autoriser l'accès à l'instance du serveur de connexion en dehors du réseau à des utilisateurs et des groupes tout en limitant l'accès pour d'autres utilisateurs et groupes.

Conditions préalables

- Un dispositif Unified Access Gateway, un serveur de sécurité ou un équilibrage de charge doivent être déployés en dehors du réseau en tant que passerelle vers l'instance du Serveur de connexion sur laquelle l'utilisateur est autorisé. Pour plus d'informations sur le déploiement d'un dispositif Unified Access Gateway, consultez le document *Déploiement et configuration d'Unified Access Gateway*.
- Les utilisateurs qui obtiennent un accès distant doivent être autorisés sur les pools de postes de travail ou d'applications.

Procédure

1. Dans la Horizon Console, sélectionnez **Utilisateurs et groupes**.
2. Cliquez sur l'onglet **Accès distant**.
3. Cliquez sur **Ajouter**, sélectionnez un ou plusieurs critères de recherche, puis cliquez sur **Rechercher** pour rechercher des utilisateurs ou des groupes en fonction de vos critères de recherche.

   Note Les utilisateurs ne disposant pas d'un accès authentifié ne s'afficheront pas dans les résultats de la recherche.
4. Pour fournir un accès distant pour un utilisateur ou un groupe ou encore un utilisateur avec accès non authentifié, sélectionnez un utilisateur ou un groupe et cliquez sur **OK**.
5. Pour supprimer un utilisateur ou un groupe de l'accès distant, sélectionnez l'utilisateur ou le groupe, cliquez sur **Supprimer**, puis sur **OK**.

Configuration de l'accès non authentifié

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.

Note L'accès non authentifié n'est pas pris en charge pour les applications publiées dans un pool de postes de travail.

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

Pour plus d'informations sur les règles et les recommandations de configuration des utilisateurs pour l'accès non authentifié, consultez le document *Administration d'Horizon 7*.

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.

Conditions préalables

- Les administrateurs ne peuvent créer qu'un seul utilisateur pour chaque compte Active Directory.
- 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.
- Si vous sélectionnez un utilisateur avec des droits de poste de travail et faites de l'utilisateur un utilisateur d'accès non authentifié, l'utilisateur n'aura pas accès aux postes de travail autorisés.

Procédure

1. Dans la Horizon Console, 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.
4. Sélectionnez un utilisateur et cliquez sur **Suivant**.
5. 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 **Envoyer**.

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 domaine, les droits d'application et les sessions.

Étape suivante

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. Reportez-vous à la section « Activer l'accès non authentifié pour des utilisateurs » dans le document *Administration d'Horizon 7*.

Activer l'accès non authentifié pour des utilisateurs de Horizon Console

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 Console, sélectionnez **Paramètres > 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**.

Étape suivante

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.

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.

Conditions préalables

- Créez une batterie de serveurs basée sur un groupe d'hôtes RDS. Pour plus d'informations sur la création de batteries de serveurs, consultez le document *Configuration d'applications et de postes de travail publiés dans Horizon Console*.
- Créez un pool d'applications pour des applications publiées exécutées sur une batterie de serveurs d'hôtes RDS. Pour plus d'informations sur la création d'applications publiées, reportez-vous à la section *Configuration d'applications et de postes de travail publiés dans Horizon Console*.

Procédure

1. Dans la Horizon Console, sélectionnez **Utilisateurs et groupes**.
2. Dans l'onglet **Droits**, sélectionnez **Ajouter une autorisation d'application** dans le menu déroulant **Droits**.
3. Cliquez sur **Ajouter**, sélectionnez un ou plusieurs critères de recherche, cochez la case **Utilisateurs non authentifiés** et cliquez sur **Rechercher** 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. Sélectionnez les applications dans le pool et cliquez sur **Envoyer**.

Étape suivante

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

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. Si vous supprimez l'utilisateur par défaut, la Horizon Console affiche un message d'erreur interne et un message de suppression réussie de l'utilisateur. Toutefois, l'utilisateur par défaut n'est pas supprimé de la Horizon Console.

Note 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 la Horizon Console, sélectionnez **Utilisateurs et groupes**.
2. Dans l'onglet **Accès non authentifié**, sélectionnez l'utilisateur et cliquez sur **Supprimer**.
3. Cliquez sur **OK**.

Étape suivante

Supprimez des droits d'application pour l'utilisateur.

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.

Conditions préalables

- 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.

Configurer des utilisateurs pour l'ouverture de session hybride dans Horizon Console

Après avoir créé un utilisateur d'accès non authentifié, vous pouvez activer l'ouverture de session hybride pour l'utilisateur. L'activation de l'ouverture de session hybride fournit aux utilisateurs d'accès non authentifié un accès de domaine à des ressources réseau, comme un partage de fichiers ou des imprimantes réseau, sans avoir à entrer les informations d'identification.

Note La fonctionnalité d'ouverture de session hybride utilise le même utilisateur de domaine pour tous les utilisateurs connectés pour un utilisateur d'accès non authentifié donné configuré pour l'ouverture de session hybride.

Note Si vous utilisez l'onglet de profil d'utilisateur pour définir le répertoire de base comme chemin d'accès réseau à partir de la machine hôte RDS, par défaut, l'interface utilisateur d'administration sur Windows supprime toutes les autorisations existantes du dossier du répertoire de base et ajoute les autorisations de l'administrateur et de l'utilisateur local avec le contrôle total. Utilisez le compte d'administrateur pour supprimer l'utilisateur local de la liste des autorisations, puis ajoutez l'utilisateur de domaine avec les autorisations que vous devez définir pour l'utilisateur.

Conditions préalables

- Vérifiez que vous avez sélectionné l'option personnalisée Ouverture de session hybride lorsque vous avez installé Horizon Agent sur l'hôte RDS. Pour plus d'informations sur les options d'installation personnalisées Horizon Agent pour un hôte RDS, consultez le document *Configuration d'applications et de postes de travail publiés dans Horizon Console*.
- Vérifiez que vous avez créé un utilisateur d'accès non authentifié. Reportez-vous à la section Créer des utilisateurs pour l'accès non authentifié.
- Vérifiez que le chiffrement DES Kerberos n'est pas activé pour le compte d'utilisateur dans le domaine. Le chiffrement DES Kerberos n'est pas pris en charge pour la fonctionnalité d'ouverture de session hybride.

Procédure

1. Dans la Horizon Console, 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 un utilisateur d'accès non authentifié correspondant à vos critères.

   L'utilisateur doit disposer d'un UPN valide.
4. Sélectionnez un utilisateur d'accès non authentifié 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. Sélectionnez **Activer l'ouverture de session hybride**.

   L'option **Activer l'authentification unique réelle** est sélectionnée par défaut. L'authentification unique réelle doit être activée pour l'environnement Horizon 7. Ensuite, les utilisateurs d'accès non authentifié pour lesquels l'ouverture de session hybride est activée utilisent l'authentification unique réelle pour se connecter à l'instance du Serveur de connexion à partir d'Horizon Client.

   Note Si l'espace du Serveur de connexion n'est pas configuré pour l'authentification unique réelle, l'utilisateur peut démarrer une application autorisée avec un accès non authentifié. Toutefois, l'utilisateur ne dispose pas de l'accès réseau, car l'authentification unique réelle n'est pas activée sur l'espace.

8 (Facultatif) Pour permettre à l'utilisateur de se connecter à l'instance du Serveur de connexion à partir d'Horizon Client, sélectionnez **Activer l'ouverture de session par mot de passe** et entrez le mot de passe de l'utilisateur.

   Utilisez ce paramètre si vous n'avez pas configuré l'authentification unique réelle pour l'environnement Horizon 7.

   Dans un environnement CPA, la fonctionnalité d'utilisateur d'ouverture de session hybride ne fonctionne que sur l'espace du Serveur de connexion sur lequel l'utilisateur d'ouverture de session hybride a été configuré avec le paramètre **Activer l'ouverture de session par mot de passe** et autorisé à accéder à des applications publiées.

   Par exemple, dans un environnement CPA avec un espace A et un espace B, l'utilisateur d'ouverture de session hybride configuré avec le paramètre **Activer l'ouverture de session par mot de passe** est autorisé à accéder à une application sur l'espace A. L'utilisateur peut consulter et démarrer l'application à partir d'un client qui se connecte à l'espace A ou à l'espace B. Toutefois, si une autre application est attribuée au même utilisateur sur l'espace B, l'utilisateur ne peut pas afficher et démarrer l'application à partir d'un client qui se connecte à l'espace B. Pour que l'ouverture de session hybride fonctionne sur l'espace B, vous devez créer un autre utilisateur d'ouverture de session hybride configuré avec le paramètre **Activer l'ouverture de session par mot de passe** et attribuer des applications à cet utilisateur. Pour plus d'informations sur la configuration d'un environnement CPA, consultez le document *Administration d'Architecture Cloud Pod dans Horizon 7*.

9 Cliquez sur **Terminer**.

Étape suivante

Autorisez l'utilisateur à accéder à des applications publiées. Reportez-vous à la section Autoriser les utilisateurs d'accès non authentifié à accéder à des applications publiées.

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 sélectionnent **Se connecter en tant qu'utilisateur actuel** dans le menu **Options**, 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 Horizon 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 utilisateur sont stockées sur l'instance du Serveur de connexion et sur le système client.

- Sur l'instance du Serveur de connexion, les informations d'identification utilisateur sont chiffrées et stockées dans la session utilisateur avec le nom d'utilisateur, le domaine et le nom d'utilisateur principal (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 Horizon LDAP ou dans un fichier de disque.

- Sur l'instance du Serveur de connexion, activez le paramètre **Autoriser l'ouverture de session en tant qu'utilisateur actuel** pour permettre à l'instance du Serveur de connexion d'accepter l'identité et les informations d'identification utilisateur qui sont transmises lorsque les utilisateurs sélectionnent **Se connecter en tant qu'utilisateur actuel** dans le menu **Options** dans Horizon Client.

  Important Vous devez comprendre les risques de sécurité avant d'activer ce paramètre. Consultez la section « Paramètres de serveur liés à la sécurité pour l'authentification utilisateur » dans le document *Sécurité d'Horizon 7*.

- 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 du paramètre **Se connecter en tant qu'utilisateur actuel** dans le menu **Options** et pour spécifier sa valeur par défaut. Les administrateurs peuvent également utiliser une stratégie de groupe pour spécifier les instances du Serveur de connexion qui acceptent l'identité et les informations d'identification de l'utilisateur qui sont transmises lorsque celui-ci sélectionne **Se connecter en tant qu'utilisateur actuel** dans Horizon Client.

La fonction de déverrouillage récursif est activée lorsqu'un utilisateur se connecte au Serveur de connexion avec la fonction Se connecter en tant qu'utilisateur actuel. Cette fonctionnalité déverrouille toutes les sessions distantes après que la machine cliente a été déverrouillée. Les administrateurs peuvent contrôler la fonction de déverrouillage récursif avec le paramètre de stratégie globale **Déverrouiller les sessions distantes lorsque la machine cliente est déverrouillée** dans Horizon Client. Pour plus d'informations sur les paramètres de stratégie globale pour Horizon Client, consultez la documentation Horizon Client dans la page Web de la documentation des clients VMware 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 requise sur une instance du Serveur de connexion, l'authentification échoue pour les utilisateurs qui sélectionnent **Se connecter en tant qu'utilisateur actuel** lorsqu'ils se connectent à cette instance. Ces utilisateurs doivent s'authentifier à nouveau avec leur carte à puce et leur code PIN lorsqu'ils se connectent au Serveur de connexion.
- L'heure du système sur lequel le client se connecte et l'heure de l'hôte du Serveur de connexion 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 du Serveur de connexion sans établir au préalable une connexion VPN, il est invité à fournir des informations d’identification, et la fonctionnalité Se connecter en tant qu'utilisateur actuel ne fonctionne pas.

Configuration de l'administration déléguée basée sur des rôles dans Horizon Console

7

Une tâche de gestion clé dans un environnement Horizon 7 consiste à déterminer qui peut utiliser Horizon Console 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 contient les rubriques suivantes :

Comprendre les rôles et les privilèges

La capacité d'effectuer des tâches dans Horizon Console 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 Horizon Console. Par exemple, si un administrateur ne dispose pas de privilèges pour voir ou modifier des stratégies générales, le paramètre **Stratégies générales** n'est pas visible dans le volet de navigation lorsque l'administrateur ouvre une session sur Horizon Console.

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. Horizon Console 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. Si le rôle contient des privilèges propres à l'objet, vous devrez appliquer le rôle à un groupe d'accès. 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 dans la Horizon Console

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 la Horizon Console. Les pools de postes de travail publiés 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.

Note Vous ne pouvez pas directement modifier le groupe d'accès d'un pool de postes de travail publiés ou d'un pool d'applications. Vous devez modifier le groupe d'accès de la batterie de serveurs à laquelle le pool de postes de travail publiés 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 la Horizon Console 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.

- Différents administrateurs pour différents groupes d'accès

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

- Différents administrateurs pour un même groupe d'accès

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

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 7-1. Différents administrateurs pour différents groupes d'accès montre un exemple de ce type de configuration.

Tableau 7-1. 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 7-2. Différents administrateurs pour un même groupe d'accès montre un exemple de ce type de configuration.

Tableau 7-2. 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 Horizon Console, 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 Horizon Console, selon que vous sélectionnez un utilisateur administrateur ou un groupe d'utilisateurs administrateurs, un groupe d'accès ou un rôle.

Le tableau suivant montre comment les autorisations apparaissent dans Horizon Console lorsque vous sélectionnez un utilisateur ou un groupe d'administrateurs. L'utilisateur administrateur est appelé Admin 1 et il possède deux autorisations.

Tableau 7-3. 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.

Le tableau suivant montre comment les mêmes autorisations s'affichent dans Horizon Console lorsque vous sélectionnez le groupe d'accès `MarketingDesktops`.

Tableau 7-4. Autorisations sous l'onglet Dossiers pour MarketingDesktops

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

La première autorisation est la même que la première autorisation indiquée dans Tableau 7-3. Autorisations sous l'onglet Administrateurs et groupes pour Admin 1. La deuxième autorisation est héritée de la deuxième autorisation indiquée dans Tableau 7-3. Autorisations sous l'onglet Administrateurs et groupes pour Admin 1. 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.

Le tableau suivant montre comment la première autorisation dans Tableau 7-3. Autorisations sous l'onglet Administrateurs et groupes pour Admin 1 s'affiche dans Horizon Console lorsque vous sélectionnez le rôle Administrateurs d'inventaire.

Tableau 7-5. Autorisations dans l'onglet Autorisations de rôle pour Administrateurs d'inventaire

Administrator	Groupe d'accès
horizon-domain.com\Admin1	`/MarketingDesktops`

Gérer des administrateurs

Les utilisateurs qui ont le rôle Administrateurs peuvent utiliser Horizon Console pour ajouter et supprimer des utilisateurs administrateurs et des groupes d'administrateurs.

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

Note Par défaut, le groupe Domain Admins est un membre du groupe Administrators local. Si vous avez spécifié le compte Administrateurs en tant que groupe Administrateurs 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 Horizon 7, vous devez supprimer le groupe Admins de domaine du groupe Administrateurs local.

- Créer un administrateur dans Horizon Console

  Pour créer un administrateur, vous sélectionnez un utilisateur ou un groupe parmi vos utilisateurs et groupes Active Directory dans Horizon Console et attribuez un rôle d'administrateur.

- Supprimer un administrateur dans Horizon Console

  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 dans Horizon Console

Pour créer un administrateur, vous sélectionnez un utilisateur ou un groupe parmi vos utilisateurs et groupes Active Directory dans Horizon Console et attribuez un rôle d'administrateur.

Conditions préalables

- Familiarisez-vous avec les rôles d'administrateur prédéfinis. Reportez-vous à la section Rôles et privilèges prédéfinis.
- 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.
- Pour affecter un rôle personnalisé à l'administrateur, créez le rôle personnalisé. Reportez-vous à la section Ajouter un rôle personnalisé dans Horizon Console.
- 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 consulter des groupes d'accès.

Procédure

1. Dans Horizon Console, accédez à **Paramètres > 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 **Appliqué 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 dans Horizon Console

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 Horizon Console, accédez à **Paramètres > 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 Horizon Console pour ajouter, supprimer et consulter des autorisations pour des utilisateurs Administrateur spécifiques et des groupes, des rôles et des groupes d'accès.

- Ajouter une autorisation dans Horizon Console

  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 dans Horizon Console

  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 les autorisations dans Horizon Console

  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 dans Horizon Console

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 Horizon Console, accédez à **Paramètres > Administrateurs**.

2 Créez l'autorisation.

Option	Action
Créer une autorisation qui inclut un utilisateur administrateur 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 d'un objet pour s'appliquer à un groupe d'accès.
Créer une autorisation qui inclut un rôle spécifique.	a Sous l'onglet **Autorisations de rôle**, 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 d'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 d'un objet pour s'appliquer à un groupe d'accès.

Supprimer une autorisation dans Horizon Console

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 Horizon Console, accédez à **Paramètres > Administrateurs**.

2 Sélectionnez l'autorisation à supprimer.

Option	Action
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**.
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 les autorisations dans Horizon Console

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

Procédure

1 Dans Horizon Console, accédez à **Paramètres > Administrateurs**.

2 Consultez les autorisations.

Option	Action
Consulter les autorisations qui comportent un administrateur ou un groupe spécifique.	Sélectionnez l'administrateur ou le groupe sous l'onglet **Administrateurs et groupes**.
Consulter les autorisations qui comportent un rôle spécifique.	Sélectionnez le rôle sous l'onglet **Autorisations de rôle** et cliquez sur **Autorisations**.
Consulter les autorisations qui incluent un groupe d'accès spécifique.	Sélectionnez le dossier dans l'onglet **Groupes d'accès**.

Gérer et consulter des groupes d'accès

Vous pouvez utiliser Horizon Console 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 dans Horizon Console

  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 dans la Horizon Console

  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 dans Horizon Console

  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 objets d'un groupe d'accès

  Vous pouvez afficher les pools de postes de travail, les pools d'applications, les batteries de serveurs ou les disques persistants d'un groupe d'accès particulier dans Horizon Console.

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

  Vous pouvez afficher les machines virtuelles vCenter incluses dans un groupe d'accès particulier dans la Horizon Console. Une machine virtuelle vCenter hérite du groupe d'accès de son pool.

Ajouter un groupe d'accès dans Horizon Console

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 la Horizon Console, accédez à la boîte de dialogue Groupe d'accès.

Option	Action
À partir des postes de travail	■ Sélectionnez **Inventaire > Postes de travail**. ■ Dans le menu déroulant **Groupe d'accès**, sélectionnez **Nouveau groupe d'accès**.
À partir des batteries de serveurs	■ Sélectionnez **Inventaire > Batteries de serveurs**. ■ Dans le menu déroulant **Groupes d'accès**, sélectionnez **Nouveau groupe d'accès**.

2 Tapez un nom et une description pour le groupe d'accès et cliquez sur **OK**.

  La description est facultative.

Étape suivante

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 dans la Horizon Console

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 la Horizon Console, sélectionnez **Inventaire > Postes de travail** ou **Inventaire > 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**.
4. Sélectionnez le groupe d'accès, puis cliquez sur **OK**.

La Horizon Console déplace le pool ou la batterie de serveurs vers le groupe d'accès que vous avez sélectionné.

Supprimer un groupe d'accès dans Horizon Console

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

Conditions préalables

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 dans la Horizon Console.

Procédure

1. Dans Horizon Console, accédez à **Paramètres > 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 objets d'un groupe d'accès

Vous pouvez afficher les pools de postes de travail, les pools d'applications, les batteries de serveurs ou les disques persistants d'un groupe d'accès particulier dans Horizon Console.

Procédure

1. Dans la Horizon Console, accédez à la page principale des objets.

Objet	Action
Pools de postes de travail	Sélectionnez **Inventaire > Postes de travail**.
Pools d'applications	Sélectionnez **Inventaire > Applications**.

Objet	Action
Batteries de serveurs	Sélectionnez **Inventaire > Batteries de serveurs**.
Disques persistants	Sélectionnez **Inventaire > Disques persistants**.

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 les machines virtuelles vCenter incluses dans un groupe d'accès particulier dans la Horizon Console. Une machine virtuelle vCenter hérite du groupe d'accès de son pool.

Procédure

1 Dans la Horizon Console, accédez à **Inventaire > 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 Horizon Console pour ajouter, modifier et supprimer des rôles personnalisés.

- Ajouter un rôle personnalisé dans Horizon Console

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

- Modifier les privilèges dans un rôle personnalisé dans Horizon Console

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

- Supprimer un rôle personnalisé dans Horizon Console

  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 dans Horizon Console

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

Conditions préalables

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.

Note Lorsque vous créez un rôle d'administrateur personnalisé, aucune autorisation globale n'est disponible pour l'utilisateur administrateur personnalisé. Seuls les rôles d'administrateur prédéfinis disposent d'autorisations globales, qui permettent la gestion des droits globaux dans un environnement Architecture Cloud Pod.

Procédure

1. Dans Horizon Console, accédez à **Paramètres > Administrateurs**.
2. Sous l'onglet **Privilèges de rôle**, cliquez sur **Ajouter un rôle**.
3. Entrez 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 dans Horizon Console

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

Conditions préalables

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.

Procédure

1. Dans Horizon Console, accédez à **Paramètres > Administrateurs**.
2. Dans l'onglet **Privilèges de rôle**, sélectionnez le rôle.
3. Affichez les Privilèges de rôle et cliquez sur **Modifier**.
4. Sélectionnez ou désélectionnez des privilèges.
5. Cliquez sur **OK** pour enregistrer vos modifications.

Supprimer un rôle personnalisé dans Horizon Console

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.

Conditions préalables

Si le rôle est inclus dans une autorisation, supprimez l'autorisation. Reportez-vous à la section Supprimer une autorisation dans Horizon Console.

Procédure

1. Dans Horizon Console, accédez à **Paramètres > Administrateurs**.
2. Sous l'onglet **Privilèges de rôle**, 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

Horizon Console comporte des rôles prédéfinis que vous pouvez attribuer 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

  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

  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

  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

  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.

Note L'attribution d'une combinaison de rôles prédéfinis ou personnalisés aux utilisateurs peut donner aux utilisateurs l'accès aux opérations qui ne sont pas possibles dans les rôles prédéfinis ou personnalisés individuels.

Le tableau suivant décrit les rôles prédéfinis et indique si un rôle peut s'appliquer à un groupe d'accès.

Tableau 7-6. Rôles prédéfinis dans Horizon Console

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 Architecture Cloud Pod, 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 votre hôte du Serveur de connexion 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 Horizon Console. ■ 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 Architecture Cloud Pod, 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 stratégies générales	Afficher et modifier des stratégies générales 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 stratégies générales (lecture seule)	Afficher, mais pas modifier, des stratégies générales et des paramètres de configuration, à l'exception des rôles et des autorisations d'administrateur, ainsi que des applications et paramètres ThinApp.	Non

Tableau 7-6. Rôles prédéfinis dans Horizon Console (suite)

Rôle	Actions réalisables par l'utilisateur	S'applique à un groupe d'accès
Administrateurs du service d'assistance	Exécuter des actions de poste de travail et d'application, telles que l'arrêt, la réinitialisation, le redémarrage, et exécuter des actions d'assistance à distance, telles que terminer les processus du poste de travail ou de l'application d'un utilisateur. Un administrateur doit disposer des autorisations sur le groupe d'accès racine pour accéder à Horizon Help Desk Tool. ■ Accès en lecture seule à Horizon Help Desk Tool. ■ Gérer les sessions globales. ■ Peut se connecter à Horizon Console. ■ Exécuter toutes les commandes liées aux machines et aux sessions. ■ Gérez les applications et les processus distants. ■ Assistance à distance du poste de travail virtuel ou du poste de travail publié.	Non
Administrateurs du service d'assistance (lecture seule)	Afficher des informations sur les utilisateurs et sur la session et explorer en détail la session. Un administrateur doit disposer des autorisations sur le groupe d'accès racine pour accéder à Horizon Help Desk Tool. ■ Accès en lecture seule à Horizon Help Desk Tool. ■ Peut se connecter à Horizon Console.	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. ■ Gérer des batteries de serveurs automatisées. 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. Les administrateurs disposant de ce rôle ne peuvent pas créer une batterie de serveurs manuelle ou un pool manuel non géré, ajouter des hôtes RDS à la batterie de serveurs ou au pool manuel non géré ni en supprimer.	Oui
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

Tableau 7-6. Rôles prédéfinis dans Horizon Console (suite)

Rôle	Actions réalisables par l'utilisateur	S'applique à un groupe d'accès
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 Architecture Cloud Pod, 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. **Note** Un administrateur avec le rôle Administrateurs locaux ne peut pas accéder à Horizon Help Desk Tool. Les administrateurs dans un environnement non-CPA ne disposent pas du privilège Gérer des sessions globales, qui est nécessaire pour effectuer des tâches dans Horizon Help Desk Tool.	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. **Note** Un administrateur avec le rôle Administrateurs locaux (lecture seule) ne peut pas accéder à Horizon Help Desk Tool. Les administrateurs dans un environnement non-CPA ne disposent pas du privilège Gérer des sessions globales, qui est nécessaire pour effectuer des tâches dans Horizon Help Desk Tool.	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.

Le tableau suivant décrit les privilèges généraux et répertorie les rôles prédéfinis qui contiennent chaque privilège.

Tableau 7-7. Privilèges généraux

Privilège	Actions réalisables par l'utilisateur	Rôles prédéfinis
Interaction de console	Connectez-vous à Horizon Console et utilisez-la. **Note** À partir de la version 7.10 d'Horizon 7, le privilège **Interaction avec la console** est automatiquement ajouté aux nouveaux rôles et n'apparaît pas dans la liste des privilèges globaux dans Horizon Console.	Administrateurs Administrateurs (lecture seule) Administrateurs d'inventaire Administrateurs d'inventaire (lecture seule) Administrateurs de configuration et stratégies générales Administrateurs de configuration et stratégies générales (lecture seule) Administrateurs de support technique Administrateurs de support technique (lecture seule) Administrateurs locaux Administrateurs locaux (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`. **Note** À partir de la version 7.10 d'Horizon 7, le privilège **Interaction directe** est automatiquement ajouté aux nouveaux rôles et n'apparaît pas dans la liste des privilèges globaux dans Horizon Console.	Administrateurs Administrateurs (lecture seule)
Gérer la configuration et les stratégies 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 stratégies générales
Gérer des sessions globales	Gérer les sessions globales dans un environnement Architecture Cloud Pod.	Administrateurs
Gérer des rôles et autorisations	Créer, modifier et supprimer des rôles et des autorisations d'administrateur.	Administrateurs

Tableau 7-7. Privilèges généraux (suite)

Privilège	Actions réalisables par l'utilisateur	Rôles prédéfinis
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.	Administrateurs Administrateurs d'inscription d'agent
Gérer la configuration de vCenter (lecture seule)	Accès en lecture seule à la configuration de vCenter Server.	Administrateurs Administrateurs (lecture seule) Administrateurs d'inventaire Administrateurs d'inventaire (lecture seule) Administrateurs locaux Administrateurs locaux (lecture seule)

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.

Le tableau suivant décrit les privilèges spécifiques de l'objet. Les rôles prédéfinis Administrators (Administrateurs) et Inventory Administrators (Administrateurs d'inventaire) contiennent tous les privilèges.

Tableau 7-8. 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 les opérations de maintenance sur les postes de travail et les batteries de serveurs automatisés	Recomposez, actualisez, rééquilibrez, planifiez une image de transfert, planifiez la maintenance et modifiez l'image par défaut d'un poste de travail et d'une batterie de serveurs.	Pool de postes de travail, batterie de serveurs
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 Horizon Composer, y compris l'attachement, le détachement et l'importation des disques persistants.	Disque persistant

Tableau 7-8. Privilèges spécifiques de l'objet (suite)

Privilège	Actions réalisables par l'utilisateur	Objet
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.

Le tableau suivant décrit les privilèges internes et répertorie les rôles prédéfinis qui contiennent chaque privilège.

Tableau 7-9. Privilèges internes

Privilège	Description	Rôles prédéfinis
Complet (lecture seule)	Accorde un accès en lecture seule à tous les paramètres.	Administrateurs (lecture seule)
Gérer l'inventaire (lecture seule)	Accorde un accès en lecture seule à des objets d'inventaire.	Administrateurs d'inventaire (lecture seule)
Gérer la configuration et les stratégies 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.	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 Horizon Console.

Le tableau suivant répertorie des tâches de gestion des pools communes et montre les privilèges requis pour effectuer chaque tâche.

Tableau 7-10. 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** **Note** Non applicable pour l'ajout d'un pool de postes de travail non géré. L'administrateur doit également disposer du rôle Administrateurs de configuration et stratégies générales (lecture seule) pour effectuer cette tâche.
Modifier ou supprimer un pool.	**Gérer des batteries de serveurs et des pools de postes de travail et d'applications** **Note** Non applicable pour la suppression d'un pool de postes de travail non géré. L'administrateur doit également disposer du rôle Administrateurs de configuration et stratégies générales (lecture seule) pour effectuer cette tâche.
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** **Note** Non applicable pour l'ajout ou la suppression de postes de travail virtuels non gérés dans le pool de postes de travail. L'administrateur doit également disposer du rôle Administrateurs de configuration et stratégies générales (lecture seule) pour effectuer cette tâche.
Actualiser, recomposer, rééquilibrer ou modifier l'image d'Horizon Console par défaut.	**Gérer l'image de pool de postes de travail de Composer** et **Gérer la configuration de vCenter (lecture seule)**.
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 posséder certains privilèges pour gérer des machines dans Horizon Console.

Le tableau suivant répertorie des tâches de gestion des machines communes et montre les privilèges requis pour effectuer chaque tâche.

Tableau 7-11. Tâches et privilèges de gestion des machines

Tâche	Privilèges requis
Supprimer une machine virtuelle.	**Gérer une machine** ou **Gérer des batteries de serveurs et des pools de postes de travail et d'applications** **Note** Non applicable pour la suppression des postes de travail non gérés ou des hôtes RDS du pool de postes de travail ou de la batterie de serveurs. L'administrateur doit également disposer du rôle Administrateurs de configuration et stratégies générales (lecture seule) pour effectuer cette tâche.
Réinitialiser une machine virtuelle.	**Gérer l'opération de redémarrage**
Redémarrer un poste de travail virtuel.	**Gérer l'opération de redémarrage**
Attribuer ou supprimer une propriété d'utilisateur.	**Gérer une machine**
Entrer dans le mode de maintenance ou le quitter.	**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 Horizon Console.

Le tableau suivant 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 Disques persistants dans Horizon Console.

Tableau 7-12. Privilèges et tâches de gestion des disques persistants

Tâche	Privilèges requis
Détacher un disque.	■ Si le disque est un disque secondaire, le privilège **Gérer des disques persistants** est nécessaire. ■ Si le disque est un disque principal, les privilèges **Gérer des disques persistants** et **Gérer une machine** sont nécessaires. ■ Pour détacher un disque sur une autre banque de données, le privilège **Gérer la configuration de vCenter (lecture seule)** est également nécessaire pour l'administrateur.
Attacher un disque.	**Gérer des disques persistants** sur le disque et **Gérer une machine** 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** ou **Gérer une machine** sur le dernier pool de postes de travail.

Tableau 7-12. Privilèges et tâches de gestion des disques persistants (suite)

Tâche	Privilèges requis
Importer depuis vCenter.	**Gérer des disques persistants** sur le disque et **Gérer la configuration de vCenter (lecture seule)**.
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 Horizon Console.

Le tableau suivant répertorie des tâches de gestion des utilisateurs et des administrateurs communes et montre les privilèges requis pour effectuer chaque tâche. Vous gérez les utilisateurs sur la page **Utilisateurs et groupes** dans Horizon Console. Vous gérez les administrateurs sur la page **Vue générale des administrateurs** dans Horizon Console.

Tableau 7-13. 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 stratégies générales**
Envoyer des messages aux utilisateurs.	**Gérer des sessions distantes** sur la machine.
Ajouter un utilisateur administrateur ou un groupe d'administrateurs.	**Gérer des rôles et autorisations**
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 les tâches de Horizon Help Desk Tool

Les administrateurs Horizon Help Desk Tool doivent disposer de certains privilèges pour effectuer des tâches de dépannage dans Horizon Console.

Le tableau suivant répertorie les tâches courantes que l'administrateur Horizon Help Desk Tool peut effectuer et indique les privilèges pour effectuer chaque tâche.

Tableau 7-14. Privilèges et tâches d'Horizon Help Desk Tool

Tâches	Privilèges requis
Accès en lecture seule à Horizon Help Desk Tool.	**Gérer le service d'assistance (lecture seule)**
Gérer les sessions globales.	**Gérer des sessions globales**
Peut se connecter à Horizon Console.	**Interaction de console** **Note** À partir de la version 7.10 d'Horizon 7, le privilège **Interaction avec la console** est automatiquement ajouté aux nouveaux rôles et n'apparaît pas dans la liste des privilèges globaux dans Horizon Console.
Exécuter toutes les commandes liées aux machines et aux sessions.	**Gérer une machine**

Tableau 7-14. Privilèges et tâches d'Horizon Help Desk Tool (suite)

Tâches	Privilèges requis
Réinitialiser ou redémarrer des machines.	**Gérer l'opération de redémarrage**
Se déconnecter et fermer des sessions.	**Gérer des sessions**
Gérez les applications et les processus distants.	**Gérer les applications et les processus distants**
Assistance à distance du poste de travail virtuel ou du poste de travail publié.	**Assistance à distance**
Opérations de déconnexion, de fermeture de session, de réinitialisation et de redémarrage pour des sessions globales.	**Gérer le service d'assistance (lecture seule)** et **Gérer des sessions globales**
Opérations de réinitialisation et de redémarrage pour des sessions locales.	**Gérer le service d'assistance (lecture seule)** et **Gérer l'opération de redémarrage**
Opérations de l'assistance à distance.	**Gérer le service d'assistance (lecture seule)** et **Assistance à distance**
Terminer les applications et les processus distants.	**Gérer le service d'assistance (lecture seule)** et **Gérer les applications et les processus distants**
Effectuer toutes les tâches dans Horizon Help Desk Tool.	**Gérer le service d'assistance (lecture seule)**, **Gérer les sessions globales**, **Gérer l'opération de redémarrage**, **Assistance à distance** et **Gérer les applications et les processus distants**
Opérations de l'assistance à distance et terminer les applications et les processus distants.	**Gérer le service d'assistance (lecture seule)**, **Assistance à distance** et **Gérer les applications et les processus distants**
Opérations de déconnexion et de fermeture de session pour des sessions locales.	**Gérer le service d'assistance (lecture seule)** et **Gérer des sessions**

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.

Le tableau suivant montre les privilèges requis pour exécuter des tâches d'administration générale et exécuter des utilitaires de ligne de commande.

Tableau 7-15. Privilèges pour des tâches et des commandes d'administration générales

Tâche	Privilèges requis
Ajouter ou supprimer un groupe d'accès	Doit disposer du rôle Administrateurs local ou Administrateurs sur le groupe d'accès racine pour supprimer un groupe d'accès. Doit disposer du rôle Administrateurs d'inventaire ou Administrateurs locaux ou Administrateurs sur le groupe d'accès racine.
Gérer des applications ThinApp et des paramètres dans Horizon Administrator	Doit disposer du rôle Administrateurs 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**

Tableau 7-15. Privilèges pour des tâches et des commandes d'administration générales (suite)

Tâche	Privilèges requis
Voir ou modifier des paramètres de configuration (sauf pour les administrateurs) dans Horizon Administrator	**Gérer la configuration et les stratégies générales**
Exécutez toutes les commandes PowerShell et les utilitaires de ligne de commande, sauf pour `vdmadmin` et `vdmimport`.	**Interaction directe** **Note** À partir de la version 7.10 d'Horizon 7, le privilège Interaction directe est automatiquement ajouté aux nouveaux rôles et n'est pas visible dans la liste des privilèges dans Horizon Console.
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.
Accès en lecture seule à la configuration de vCenter Server.	**Gérer la configuration de vCenter (lecture seule)**

Meilleures pratiques pour des utilisateurs et des groupes d'administrateurs

Pour augmenter la sécurité et la gérabilité de votre environnement Horizon 7, 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 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 Horizon 7 ou qui ne devraient pas en disposer.
- Maintenez à un minimum le nombre d'utilisateurs disposant de privilèges administratifs Horizon 7.
- 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 Horizon 7.

Définition de stratégies dans Horizon Console

8

Vous utilisez Horizon Console pour configurer des stratégies pour les sessions clientes.

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.

Note Seules les stratégies générales sont disponibles pour les pools de postes de travail et d'applications publiés. Vous ne pouvez pas définir des stratégies de niveau utilisateur ou des stratégies de niveau pool pour les pools de postes de travail et d'applications publiés.

Ce chapitre contient les rubriques suivantes :

Configurer des stratégies générales

Vous pouvez configurer des règles générales pour contrôler le comportement de tous les utilisateurs de sessions client.

Procédure

1 Dans Horizon Console, sélectionnez **Paramètres > Stratégies générales**.

Le volet **Stratégies générales** affiche les paramètres qui affectent l'ensemble des sessions client, des pools de postes de travail ou des utilisateurs.

Tableau 8-1. Stratégies Horizon

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**.

2 Cliquez sur **Modifier les stratégies** pour modifier les paramètres.

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

Maintenance de composants Horizon 7

9

Pour garder vos composants Horizon 7 disponibles et exécutés, vous pouvez effectuer diverses tâches de maintenance.

Ce chapitre contient les rubriques suivantes :

Sauvegarde et restauration de données de configuration d'Horizon 7

Vous pouvez sauvegarder vos données de configuration d'Horizon 7 et d'Horizon Composer en planifiant ou en exécutant des sauvegardes automatiques dans Horizon Console. Vous pouvez restaurer votre configuration d'Horizon 7 en important manuellement les fichiers View LDAP et les fichiers de base de données Horizon Composer sauvegardés.

Vous pouvez utiliser les fonctionnalités de sauvegarde et de restauration pour conserver et migrer des données de configuration de Horizon 7.

Sauvegarde des données du Serveur de connexion Horizon et d'Horizon Composer

Après avoir terminé la configuration initiale du Serveur de connexion, vous devez planifier des sauvegardes régulières de vos données de configuration d'Horizon 7 et d'Horizon Composer. Vous pouvez conserver vos données d'Horizon 7 et d'Horizon Composer à l'aide d'Horizon Console.

Horizon 7 stocke des données de configuration du Serveur de connexion dans le référentiel View LDAP. Horizon Composer stocke les données de configuration des postes de travail de clone lié dans la base de données Horizon Composer.

Lorsque vous utilisez Horizon Console pour effectuer des sauvegardes, Horizon 7 sauvegarde les données de configuration de View LDAP et la base de données Horizon 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 une description de View LDAP, reportez-vous à la section « Annuaire View LDAP » dans le document *Administration d'Horizon 7*.

Vous pouvez effectuer les sauvegardes de plusieurs façons.

- Planifiez des sauvegardes automatiques en utilisant la fonctionnalité Sauvegarde de configuration de Horizon 7.
- Initiez une sauvegarde immédiatement en utilisant la fonctionnalité **Sauvegarder maintenant** dans Horizon Console.
- Exportez manuellement des données View LDAP en utilisant l'utilitaire `vdmexport`. Cet utilitaire est fourni avec chaque instance du Serveur de connexion.

  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.

  Note L'outil `vdmexport` sauvegarde uniquement les données View LDAP. Cette commande ne sauvegarde pas les informations sur la base de données Horizon Console.

  Pour plus d'informations sur `vdmexport`, reportez-vous à la section Exporter des données de configuration depuis le Serveur de connexion Horizon.

Les recommandations suivantes s'appliquent à la sauvegarde des données de configuration de Horizon 7 :

- Horizon 7 peut exporter des données de configuration de n'importe quelle instance du Serveur de connexion.
- Si vous possédez plusieurs instances du Serveur de connexion 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 à ce que des instances répliquées du Serveur de connexion agissent comme votre mécanisme de sauvegarde. Lorsqu'Horizon 7 synchronise des données dans des instances répliquées du Serveur de connexion, toutes les données perdues dans une instance peuvent être perdues dans tous les membres du groupe.

- Si le Serveur de connexion utilise plusieurs instances de vCenter Server avec plusieurs services Horizon Composer, Horizon 7 sauvegarde toutes les bases de données Horizon Composer associées aux instances de vCenter Server.

Planifier des sauvegardes de configuration de Horizon 7

Vous pouvez planifier la sauvegarde de vos données de configuration de Horizon 7 à intervalles réguliers. Horizon 7 sauvegarde le contenu du référentiel View LDAP dans lequel vos instances du Serveur de connexion stockent leurs données de configuration.

Vous pouvez sauvegarder la configuration immédiatement en sélectionnant l'instance du Serveur de connexion et en cliquant sur **Sauvegarder maintenant**.

Conditions préalables

Familiarisez-vous avec les paramètres de sauvegarde. Reportez-vous à la section Paramètres de sauvegarde de configuration d'Horizon 7.

Procédure

1. Dans Horizon Console, sélectionnez **Paramètres > Serveurs**.
2. Dans l'onglet **Serveurs de connexion**, sélectionnez l'instance du Serveur de connexion à sauvegarder et cliquez sur **Sauvegarder maintenant**.
3. Dans l'onglet **Sauvegarder**, spécifiez les paramètres de sauvegarde de configuration de Horizon 7 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'Horizon 7

Horizon 7 peut sauvegarder vos données de configuration du Serveur de connexion et d'Horizon Composer à intervalles réguliers. Dans Horizon Console, vous pouvez définir la fréquence et d'autres aspects des opérations de sauvegarde.

Tableau 9-1. Paramètres de sauvegarde de configuration d'Horizon 7

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.
Heure de sauvegarde	Heure de planification d'une sauvegarde.
Décalage du temps de sauvegarde	Décalage du temps d'une sauvegarde planifiée.
Nombre max. de sauvegardes	Nombre de fichiers de sauvegarde pouvant être stockés sur l'instance du Serveur de connexion. Le nombre doit être un entier supérieur à 0. Lorsque le nombre maximal est atteint, Horizon 7 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 s'exécute : `C:\Programdata\VMware\VDM\backups` Lorsque vous utilisez l'option **Sauvegarder maintenant**, Horizon 7 stocke également les fichiers de sauvegarde à cet emplacement.

Exporter des données de configuration depuis le Serveur de connexion Horizon

Vous pouvez sauvegarder des données de configuration d'une instance du Serveur de connexion Horizon 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. Si vous possédez plusieurs instances du Serveur de connexion dans un groupe répliqué, vous devez uniquement exporter les données depuis une seule instance. Toutes les instances répliquées contiennent les mêmes données de configuration.

Note La commande `vdmexport.exe` sauvegarde uniquement les données View LDAP. Cette commande ne sauvegarde pas les informations sur la base de données Horizon Composer.

Conditions préalables

- Recherchez le fichier exécutable de la commande `vdmexport.exe` installé avec le Serveur de connexion dans le chemin par défaut.

  `C:\Program Files\VMware\VMware View\Server\tools\bin`

- Ouvrez une session sur une instance du Serveur de connexion en tant qu'utilisateur dans le rôle Administrateurs ou Administrateurs (lecture seule).

Procédure

1. Sélectionnez **Démarrer > Invite de commande**.
2. À l'invite de commande, saisissez la commande `vdmexport` et redirigez la sortie vers un fichier. Par exemple :

   ```
   vdmexport > Myexport.LDF
   ```

   Par défaut, les données exportées sont cryptées.

   Vous pouvez spécifier le nom du fichier de sortie comme argument de l'option `–f`. Par exemple :

   ```
   vdmexport –f Myexport.LDF
   ```

   Vous pouvez exporter les données au format de texte brut (textuel) à l'aide de l'option `–v`. Par exemple :

   ```
   vdmexport –f Myexport.LDF –v
   ```

   Vous pouvez exporter les données au format de texte brut avec mots de passe et données sensibles supprimés (nettoyé) à l'aide de l'option `–c`. Par exemple :

   ```
   vdmexport –f Myexport.LDF –c
   ```

   Note N'envisagez pas d'utiliser des données de sauvegarde nettoyées pour restaurer une configuration View LDAP. Les données de configuration nettoyées ne contiennent pas les mots de passe et autres informations critiques.

Pour plus d'informations sur la commande `vdmexport`, consultez le document *Intégration d'Horizon 7*.

Étape suivante

Vous pouvez restaurer ou transférer les informations de configuration du Serveur de connexion 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 du Serveur de connexion Horizon et d'Horizon Composer

Restauration des données de configuration du Serveur de connexion Horizon et d'Horizon Composer

Vous pouvez restaurer manuellement les fichiers de configuration LDAP du Serveur de connexion et les fichiers de base de données Horizon Composer qui ont été sauvegardés par Horizon 7.

Vous exécutez manuellement des utilitaires séparés pour restaurer les données de configuration du Serveur de connexion et d'Horizon Composer.

Avant de restaurer des données de configuration, vérifiez que vous avez sauvegardé les données de configuration dans Horizon Console. Reportez-vous à la section Sauvegarde des données du Serveur de connexion Horizon et d'Horizon Composer.

Vous utilisez l'utilitaire `vdmimport` pour importer les données du Serveur de connexion des fichiers de sauvegarde LDIF vers le référentiel View LDAP dans l'instance du Serveur de connexion.

Vous pouvez utiliser l'utilitaire `SviConfig` pour importer les données d'Horizon Composer des fichiers de sauvegarde `.svi` vers la base de données SQL d'Horizon Composer.

Note Dans certains cas, il peut s'avérer nécessaire d'installer la version actuelle d'une instance du Serveur de connexion et de restaurer la configuration existante d'Horizon 7 en important les fichiers de configuration LDAP du Serveur de connexion. 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 Horizon 7 ou pour d'autres raisons. Pour plus d'informations, reportez-vous au document *Installation d'Horizon 7*.

Importer des données de configuration dans le Serveur de connexion Horizon

Vous pouvez restaurer des données de configuration d'une instance du Serveur de connexion 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.

Si vous avez sauvegardé votre configuration View LDAP à l'aide d'Horizon Console 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.

Note 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 Horizon et d'Horizon Composer

Conditions préalables

- Recherchez le fichier exécutable de la commande `vdmimport` installé avec le Serveur de connexion dans le chemin par défaut.

  `C:\Program Files\VMware\VMware View\Server\tools\bin`

- Connectez-vous à une instance du Serveur de connexion en tant qu'utilisateur avec le 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 d'Horizon Composer en arrêtant le service VMware Horizon Composer for Windows sur les serveurs sur lequel s'exécute Horizon Composer.
2. Désinstallez toutes les instances du Serveur de connexion Horizon.

   Désinstallez le Serveur de connexion VMware Horizon et AD LDS Instance VMwareVDMDS.
3. Installez une instance du Serveur de connexion.
4. Arrêtez l'instance du Serveur de connexion en arrêtant le service Windows Serveur de connexion VMware Horizon.
5. Cliquez sur **Démarrer > Invite de commande**.
6. 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 :

   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.
7. Importez le fichier LDIF décrypté pour restaurer la configuration View LDAP.

   Spécifiez l'option `–f` avec le fichier LDIF décrypté. Par exemple :
8. Désinstallez le Serveur de connexion.

   Désinstallez uniquement le module Serveur de connexion VMware Horizon.
9. Réinstallez le Serveur de connexion.
10. Connectez-vous à Horizon Console et vérifiez que la configuration est correcte.
11. Démarrez les instances d'Horizon Composer.
12. Réinstallez les instances du serveur réplica.

La commande `vdmimport` met à jour le référentiel View LDAP dans le Serveur de connexion avec les données de configuration du fichier LDIF. Pour plus d'informations sur la commande `vdmimport`, consultez le document *Installation d'Horizon 7*.

Note Assurez-vous que la configuration qui est restaurée correspond aux machines virtuelles qui sont connues de vCenter Server et d'Horizon Composer, s'il est utilisé. Si nécessaire, restaurez la configuration d'Horizon Composer à partir d'une sauvegarde. Reportez-vous à la section Restaurer une base de données Horizon Composer. Après la restauration de la configuration d'Horizon Composer, vous devrez peut-être résoudre manuellement des incohérences si les machines virtuelles dans vCenter Server ont changé depuis la sauvegarde de la configuration d'Horizon Composer.

Restaurer une base de données Horizon Composer

Vous pouvez importer les fichiers de sauvegarde pour votre configuration Horizon Composer dans la base de données Horizon Composer qui stocke les informations de clone lié.

Vous pouvez utiliser la commande `SviConfig restoredata` pour restaurer les données de base de données Horizon Composer après une panne du système ou pour rétablir la configuration d'Horizon Composer à un état précédent.

Important Seuls les administrateurs Horizon Composer expérimentés doivent utiliser l'utilitaire `SviConfig`. Cet utilitaire est conçu pour résoudre des problèmes liés au service Horizon Composer.

Conditions préalables

Vérifiez l'emplacement des fichiers de sauvegarde de la base de données Horizon Composer. Par défaut, Horizon 7 stocke les fichiers de sauvegarde sur le lecteur `C:` de l'ordinateur Serveur de connexion, dans le répertoire `C:\Programdata\VMWare\VDM\backups`.

Les fichiers de sauvegarde d'Horizon Composer utilisent une convention de dénomination avec un horodatage et un 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 Horizon 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 Horizon Composer de l'ordinateur Serveur de connexion vers un emplacement qui est accessible à l'ordinateur sur lequel le service VMware Horizon Composer est installé.
2. Sur l'ordinateur sur lequel Horizon Composer est installé, arrêtez le service VMware Horizon Composer.
3. Ouvrez une invite de commande Windows et accédez au fichier exécutable `SviConfig`.

   Le fichier est situé avec l'application Horizon 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 Composer.

Étape suivante

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 Horizon Console.

Codes de résultat pour la restauration de la base de données Horizon Console

Lorsque vous restaurez une base de données Horizon Console, la commande `SviConfig restoredata` affiche un code de résultat.

Tableau 9-2. 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.

Tableau 9-2. Codes de résultat de restoredata (suite)

Code	Description
4	Problème inattendu et échec de la commande.
14	Une autre application utilise le service VMware Horizon Console. 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 Horizon Composer

Vous pouvez exporter des données depuis votre base de données Horizon Composer vers un fichier.

Important Utilisez l'utilitaire `SviConfig` uniquement si vous êtes un administrateur Horizon Composer expérimenté.

Conditions préalables

Par défaut, Horizon 7 stocke les fichiers de sauvegarde sur le lecteur `C:` de l'ordinateur Serveur de connexion, dans le répertoire `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 Horizon Composer est installé, arrêtez le service VMware Horizon Composer.
2. Ouvrez une invite de commande Windows et accédez au fichier exécutable `SviConfig`.

   Le fichier est situé avec l'application Horizon Composer.

   Horizon_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_Horizon_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"
```

Étape suivante

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 Horizon Composer.

Codes de résultat pour l'exportation de la base de données Horizon Composer

Lorsque vous exportez une base de données Horizon Composer, la commande `SviConfig exportdata` affiche un code de sortie.

Tableau 9-3. 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.

Surveiller les composants Horizon 7

Vous pouvez rapidement contrôler l'état des composants Horizon 7 et vSphere dans votre déploiement Horizon 7 à l'aide du tableau de bord de Horizon Console.

Horizon Console affiche des informations de contrôle sur des instances du Serveur de connexion, la base de données des événements, des passerelles, des services Horizon Composer, des banques de données, des instances de vCenter Server et des domaines.

Note Horizon 7 ne peut pas déterminer des informations d'état sur les domaines Kerberos. Horizon Console affiche l'état du domaine Kerberos comme inconnu, même lorsqu'un domaine est configuré et fonctionne.

Procédure

1 Dans Horizon Console, accédez à **Surveiller > Tableau de bord**.

2 Dans le volet **Intégrité du système**, cliquez sur **Afficher**.

Le volet Détails affiche le nom, la version et d'autres informations relatives à chaque problème.

- Une coche verte indique qu'un composant n'a pas de problème.
- Un point d'exclamation rouge indique qu'un composant n'est pas disponible ou qu'il ne fonctionne pas.
- Un point d'exclamation 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 Effectuez une sélection pour afficher des informations supplémentaires sur un problème.

Option	Description
Composants	Affiche des informations sur les composants de service. Cliquez sur **Serveurs de connexion**, **Serveurs de passerelle**, **Base de données des événements**, **Serveurs View Composer** ou **Authentification unique réelle** pour afficher des informations sur les composants de service et effectuer des tâches de dépannage. Sélectionnez un composant pour effectuer les tâches suivantes : ■ Affichez l'état, le nom, la version et d'autres détails. ■ Si vous sélectionnez un Serveur de connexion, cliquez sur l'onglet **Afficher l'état des services** pour afficher des informations sur les services de passerelle. ■ Si vous sélectionnez un Serveur de connexion, cliquez sur l'onglet **Afficher les détails des sessions** pour afficher des informations sur les sessions du Serveur de connexion.
Batteries de serveurs RDS	Affiche des informations sur les batteries de serveurs. Cliquez sur un ID de batterie de serveurs pour afficher des informations supplémentaires sur la batterie de serveurs, y compris sur les hôtes RDS qui appartiennent à la batterie de serveurs.
vSphere	Affiche des informations sur les composants associés à vSphere. Cliquez sur les volets **Banques de données**, **Hôtes ESX** et **Serveurs vCenter** pour afficher des informations sur chaque composant.

Option	Description
Autres composants	Cliquez sur les onglets **Domaines**, **SAML 2.0** et **Service de licence** pour afficher des informations complémentaires sur chaque composant. Cette section s'applique également à Horizon Composer. **Note** Si un authentificateur SAML 2.0 affiche un avertissement en raison d'un certificat non approuvé, vous pouvez cliquer sur le lien du certificat pour accepter et valider le certificat.
Espaces distants	Affiche des informations sur les espaces Horizon 7 distants. **Note** Cette section apparaît uniquement lorsque la fonctionnalité Architecture Cloud Pod est activée.

4 Dans le volet **Sessions**, vous pouvez afficher les graphiques à barres qui indiquent le nombre de sessions actives, déconnectées ou inactives des postes de travail virtuels, des postes de travail publiés et des applications publiées.

5 Dans le volet **Sessions**, cliquez sur **Afficher** pour afficher les sessions.

La page Sessions contient des informations sur les sessions.

6 Dans le volet **Charge de travail**, cliquez sur **Afficher** pour afficher les banques de données.

Vous pouvez sélectionner une banque de données pour afficher des détails supplémentaires, tels que l'utilisation actuelle de la banque de données. Horizon Console affiche un avertissement si l'espace libre d'une banque de données dépasse une valeur seuil. S'il existe des pools de postes de travail associés à une banque de données sélectionnée, vous pouvez afficher les informations des pools de postes de travail lorsque vous sélectionnez la banque de données. La colonne **Autres banques de données** contient des informations sur les pools de postes de travail qui s'étendent sur plusieurs banques de données.

Surveiller l'état de charge du Serveur de connexion Horizon

Vous pouvez surveiller la charge d'un Serveur de connexion dans le tableau de bord Horizon Console. Pour chaque Serveur de connexion, vous pouvez afficher le pourcentage de CPU et de mémoire utilisé, le nombre de sessions de protocole d'affichage, de sessions de connexion du Serveur de connexion ou le seuil pour le nombre maximal de sessions pouvant se connecter à un Serveur de connexion. Vous pouvez également afficher le nombre de sessions connectées pour un hôte RDS.

Procédure

1 Dans Horizon Console, accédez à **Surveiller > Tableau de bord**.

2 Dans le volet **Intégrité du système**, cliquez sur **Afficher**.

Dans le volet **Composants**, dans l'onglet **Serveurs de connexion**, la colonne **Sessions** affiche le pourcentage de sessions du Serveur de connexion pour chaque Serveur de connexion. La colonne **Consommation du CPU** affiche le pourcentage de CPU consommé pour chaque Serveur de connexion. La colonne **Consommation de la mémoire** affiche le pourcentage de mémoire utilisée pour chaque Serveur de connexion.

Note Si le Serveur de connexion n'est pas configuré avec une connexion de passerelle sécurisée avec le tunnel sécurisé HTTP (s), PCoIP Secure Gateway et les connexions Blast Secure Gateway, Horizon Console n'affiche pas de pourcentage de sessions du Serveur de connexion et répertorie le nombre de sessions du Serveur de connexion.

3 Sélectionnez un Serveur de connexion et cliquez sur **Afficher les détails des sessions** pour afficher les sessions du Serveur de connexion, le nombre maximal de sessions du Serveur de connexion et afficher les sessions du protocole d'affichage.

Note Si le Serveur de connexion n'est pas configuré avec une connexion de passerelle sécurisée avec le tunnel sécurisé HTTP (s), PCoIP Secure Gateway et les connexions Blast Secure Gateway, Horizon Console n'affiche pas le seuil de session maximal, car il n'existe aucun seuil sur le nombre de sessions pouvant se connecter au Serveur de connexion.

4 Pour afficher le nombre de sessions sur un hôte RDS, dans le volet **Composants**, cliquez sur **Batteries de serveurs RDS**, puis cliquez sur un ID de batterie de serveurs.

La colonne Sessions affiche le nombre de sessions sur un hôte RDS.

Surveiller les services sur le Serveur de connexion Horizon

Vous pouvez surveiller les composants de service de passerelle exécutés sur un Serveur de connexion dans le tableau de bord Horizon Console. Les composants du service de passerelle incluent une connexion Secure Gateway configurée avec un tunnel sécurisé HTTP (s), une passerelle PCoIP et des connexions Blast Secure Gateway.

Procédure

1 Dans Horizon Console, accédez à **Surveiller > Tableau de bord**.

2 Dans le volet **Intégrité du système**, cliquez sur **Afficher**.

3 Sélectionnez un Serveur de connexion, puis **Afficher l'état des services View**.

La boîte de dialogue **État des services de passerelle** affiche l'état des composants du service de passerelle et des composants du service de passerelle en cours d'utilisation.

Note Les composants de service qui ne sont pas activés apparaissent grisés.

Présentation des services Horizon 7

Le fonctionnement d'instances du Serveur de connexion 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 Horizon 7. Si vous arrêtez les services Horizon 7 sur un hôte du Serveur de connexion 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 Horizon 7 qu'il contrôle ne répond plus.

Arrêter et démarrer les services Horizon 7

Le fonctionnement d'instances du Serveur de connexion 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 Horizon 7.

Lorsque vous arrêtez les services Horizon 7, 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.

Note Arrêtez uniquement le service VMware Horizon View Connection Server sur un hôte du Serveur de connexion ou le service Serveur de sécurité VMware Horizon View sur un serveur de sécurité. N'arrêtez pas d'autres services de composant.

Conditions préalables

Familiarisez-vous avec les services exécutés sur les hôtes du Serveur de connexion et les serveurs de sécurité comme expliqué dans les sections Services sur un hôte du Serveur de connexion et Services sur un serveur de sécurité.

Procédure

1. Démarrez l'outil Windows Services en saisissant **`services.msc`** à l'invite de commande.
2. Sélectionnez le service VMware Horizon View Connection Server sur un hôte du Serveur de connexion ou le service Serveur de sécurité VMware Horizon 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

Le fonctionnement d'Horizon 7 dépend de plusieurs services s'exécutant sur un hôte du Serveur de connexion.

Tableau 9-4. Services d'un hôte du Serveur de connexion Horizon

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 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 Horizon 7. 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 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 d'Horizon 7, ce service garantit la migration correcte des données existantes.

Services sur un serveur de sécurité

Le fonctionnement de Horizon 7 dépend de plusieurs services s'exécutant sur un serveur de sécurité.

Tableau 9-5. 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 9-5. 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 ou les modes de licence dans Horizon Console

Si la licence d'un système expire ou si vous souhaitez accéder à des fonctionnalités d'Horizon 7 qui ne sont pas actuellement sous licence, utilisez Horizon Console pour modifier la clé de licence produit. En fonction de votre déploiement d'Horizon 7 sur VMware Horizon Cloud Service, vous pouvez obtenir une licence perpétuelle ou une licence d'abonnement pour Horizon 7. Vous pouvez utiliser Horizon Console pour modifier le mode de licence d'une licence d'abonnement à une licence perpétuelle et vice versa pour un espace.

Vous pouvez ajouter une licence à Horizon 7 pendant l'exécution de Horizon 7. Vous n'avez pas à redémarrer le système, et l'accès aux postes de travail et aux applications n'est pas interrompu.

Conditions préalables

- Pour qu'Horizon 7 et des fonctionnalités complémentaires, telles qu'Horizon Composer et des applications publiées, fonctionnent correctement, obtenez une clé de licence produit valide.
- Pour utiliser une licence d'abonnement, vérifiez que vous activez Horizon 7 pour une licence d'abonnement. Reportez-vous au document *Installation d'Horizon 7*. Le volet **Licence** affiche des informations sur la licence d'abonnement pour l'espace Horizon 7.

Procédure

1. Dans Horizon Console, sélectionnez **Paramètres > 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. Pour modifier la clé de licence, cliquez sur **Modifier la licence**, entrez le numéro de série de la licence et cliquez sur **OK**.

   Le volet **Paramètres de licence** affiche les informations de licence mises à jour.

3 (Facultatif) Pour passer d'une licence d'abonnement à une licence perpétuelle pour un espace Horizon 7, cliquez sur **Utiliser une licence perpétuelle** et cliquez sur **OK**.

   Le volet **Paramètres de licence** affiche les informations de licence mises à jour.

4 (Facultatif) Pour passer d'une licence perpétuelle à une licence d'abonnement pour un espace Horizon 7, cliquez sur **Utiliser une licence d'abonnement** et cliquez sur **OK**. L'administrateur VMware Horizon Cloud Service peut ensuite activer l'espace Horizon 7 pour une licence d'abonnement.

   Le volet **Paramètres de licence** affiche les informations de licence mises à jour.

5 Vérifiez la date d'expiration de la licence.

6 Vérifiez que les licences d'utilisation à distance des postes de travail et des applications, et d'Horizon 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.

7 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

Dans Horizon Console, vous pouvez surveiller les utilisateurs actifs connectés simultanément à Horizon 7. Le volet **Paramètres d'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.

Horizon 7 fournit deux modèles d'utilisation de licences, un pour les utilisateurs nommés et l'autre pour les utilisateurs simultanés. Horizon 7 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, Horizon 7 compte le nombre d'utilisateurs uniques qui ont accédé à l'environnement Horizon 7. Si un utilisateur nommé exécute plusieurs postes de travail mono-utilisateur, des postes de travail publiés et des applications publiées, l'utilisateur est compté une fois.

Pour les utilisateurs nommés, la colonne **Actuel** du volet **Paramètres d'utilisation** affiche le nombre d'utilisateurs depuis la première configuration de votre déploiement d'Horizon 7 ou depuis la dernière réinitialisation du nombre d'utilisateurs nommés. La colonne **Maximum** ne s'applique pas aux utilisateurs nommés.

Pour les utilisateurs simultanés, Horizon 7 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 publiés sont comptées par utilisateur. Si un utilisateur simultané exécute plusieurs sessions de poste de travail publiés et plusieurs applications, l'utilisateur n'est compté qu'une fois, même si différents postes de travail ou applications publiés sont hébergés sur différents hôtes RDS. Si un utilisateur simultané exécute un poste de travail mono-utilisateur et des postes de travail et applications publiés supplémentaires, l'utilisateur n'est compté qu'une fois.

Pour les utilisateurs simultanés, la colonne **Maximum** du volet **Paramètres d'utilisation** affiche le nombre maximal de sessions de poste de travail simultanées et d'utilisateurs de postes de travail et d'applications publiés depuis la première configuration de votre déploiement d'Horizon 7 ou depuis la dernière réinitialisation du nombre maximal.

Vous pouvez surveiller le nombre de sessions de collaboration et de collaborateurs de session connectés à une session.

- Actif - sessions de collaboration : nombre de sessions où un propriétaire de session a invité un ou plusieurs utilisateurs à rejoindre une session. Exemple : John a invité deux personnes à rejoindre sa session et Marie a invité à une personne à rejoindre sa session. La valeur de cette ligne est 2, que l'un des invités ait rejoint la session ou non.
- Actif - nombre total de collaborateurs : nombre total d'utilisateurs qui sont connectés à une session de collaboration, y compris le propriétaire de la session et des collaborateurs. Exemple : John a invité deux personnes et une seule personne a rejoint la session. Marie a invité à une personne qui n'a pas rejoint la session. La valeur de cette ligne est 3 : la session collaborative de John dispose d'un collaborateur principal et d'un collaborateur secondaire, alors que la session collaborative de Marie dispose d'un collaborateur principal et d'aucun collaborateur secondaire. Comme le propriétaire de la session est compté, le nombre total de collaborateurs est forcément toujours supérieur ou égal au nombre total de sessions de collaboration.

Réinitialiser les données d'utilisation des licences

Dans Horizon Console, 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.

Conditions préalables

Familiarisez-vous avec l'utilisation des licences produit. Reportez-vous à la section Surveillance de l'utilisation des licences.

Procédure

1 Dans Horizon Console, sélectionnez **Paramètres > 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**.

Participer au programme d'amélioration du produit

Vous pouvez configurer Horizon 7 pour participer au programme d'amélioration du produit VMware (CEIP).

Pour plus d'informations sur le type de données que VMware recueille dans le CEIP et sur la manière dont VMware utilise ces données, consultez le Centre d'approbation et d'assurance à l'adresse http://www.vmware.com/trustvmware/ceip.html.

Pour configurer le partage de données dans Horizon Client, consultez le Guide d'installation et de configuration de Horizon Client approprié. Par exemple, pour les clients Windows, consultez le document *Guide d'installation et de configuration de VMware Horizon Client pour Windows*. Pour configurer le partage de données dans HTML Access, reportez-vous au document *Guide d'installation et de configuration de VMware Horizon HTML Access*.

Procédure

1 Dans Horizon Console, sélectionnez **Paramètres > Licence produit et utilisation**.

2 Sélectionnez l'onglet **Programme d'expérience utilisateur** et cliquez sur **Modifier les paramètres**.

3 Pour participer au programme d'amélioration du produit, sélectionnez **Participer au programme d'amélioration du produit VMware**.

   Si vous ne sélectionnez pas cette option, vous ne pouvez pas participer au CEIP.

4 (Facultatif) Sélectionnez votre emplacement géographique, votre secteur d'activité ou le nombre d'employés de votre entreprise.

5 Cliquez sur **OK**.

Intégration du Serveur de connexion Horizon au dispositif Skyline Collector

Vous pouvez configurer le Serveur de connexion Horizon afin qu'il s'intègre au dispositif Skyline Collector, que le support technique de VMware utilise pour diagnostiquer et résoudre les problèmes avec Horizon 7. Le dispositif Skyline Collector extrait les journaux du Serveur de connexion pour l'utilisateur administrateur Horizon 7 configuré pour la collecte de journaux.

Procédure

1 Dans Horizon Console, créez un rôle personnalisé nommé Administrateurs de collecteur de journaux avec le privilège Collecter des journaux d'opérations. Reportez-vous à la section Ajouter un rôle personnalisé dans Horizon Console.

2 Ajoutez une description pour le rôle personnalisé.

3 Ajoutez un nouvel utilisateur administrateur et choisissez le rôle Administrateur d'inventaire (lecture seule) et le rôle personnalisé Administrateurs de collecteur de journaux pour l'utilisateur.

Le dispositif Skyline Collector peut extraire les journaux du Serveur de connexion pour cet utilisateur administrateur afin de diagnostiquer et de résoudre des problèmes liés à Horizon 7.

Prise en main de JMP Integrated Workflow

10

Familiarisez-vous avec les concepts généraux de JMP Integrated Workflow et terminez les tâches requises pour commencer à utiliser les fonctionnalités de JMP Integrated Workflow.

Ce chapitre contient les rubriques suivantes :

À propos de JMP Integrated Workflow

Avec les fonctionnalités de VMware HorizonJMP (Just-in-Time Management Platform) Integrated Workflow, vous pouvez utiliser une console unique pour définir et gérer des espaces de travail de poste de travail pour des utilisateurs ou un groupe d'utilisateurs.

Un espace de travail de poste de travail est créé en définissant une attribution JMP qui inclut des informations sur les paramètres des pools de postes de travail VMware Horizon, des AppStacks VMware App Volumes et de VMware Dynamic Environment Manager. Une fois l'attribution JMP envoyée, le moteur d'automatisation JMP communique avec les systèmes Horizon 7, App Volumes et Dynamic Environment Manager pour attribuer l'utilisateur à un poste de travail.

Vous pouvez gérer les attributions JMP existantes à l'aide de l'onglet **Attributions (JMP)** dans la Horizon Console. Vous pouvez également modifier l'attribution de chaque composant à l'aide de la console du composant JMP respective. Par exemple, les modifications apportées aux pools de postes de travail définis dans une attribution JMP peuvent également être appliquées en sélectionnant **Inventaire > Postes de travail** dans la Horizon Console.

Lorsqu'une attribution JMP est ouverte dans la Horizon Console, l'état actuel de chaque composant de l'attribution JMP est validé pour vous assurer qu'il est dans l'état attendu. Lorsque des différences sont identifiées, les zones affectées sont mises en surbrillance dans la console et vous pouvez accepter l'état actuel ou modifier l'attribution pour atteindre l'état souhaité et autoriser de nouveau l'utilisateur.

Les fonctionnalités de JMP Integrated Workflow deviennent disponibles dans la Horizon Console une fois que vous installez et configurez VMware HorizonJMP Server. Reportez-vous à la section Prise en main de JMP Integrated Workflow et au *Guide d'installation et de configuration de VMware Horizon JMP Server* pour plus d'informations.

Note Les fonctionnalités de JMP Integrated Workflow ne prennent pas en charge VMware Cloud® on AWS, car App Volumes ne prend pas en charge VMware Cloud.

Prise en main de JMP Integrated Workflow

Pour commencer à utiliser les fonctionnalités de JMP Integrated Workflow, vous devez installer et configurer JMP Server et définir les paramètres JMP.

Conditions préalables

Passez en revue les conditions préalables et la configuration système requise pour tous les composants de la technologie que vous prévoyez d'installer.

Procédure

1. Si nécessaire, configurez les utilisateurs et les groupes d'administrateurs requis dans Active Directory.

   Reportez-vous à la section « Préparation d'Active Directory » dans le document *Installation d'Horizon 7*. Les informations Active Directory sont requises lorsque vous configurez les paramètres JMP.

2. Configurez Microsoft SQL Server et assurez-vous que les informations d'identification de connexion que vous prévoyez d'utiliser lors du processus d'installation de JMP Server ont été créées. Reportez-vous à la section « Exigences de base de données pour JMP Server » dans le document *Guide d'installation et de configuration de VMware Horizon JMP Server* pour plus d'informations.

3. Installez et configurez VMware Horizon 7 version 7.5 ou ultérieure.

   Reportez-vous au document *Installation d'Horizon 7*.

4. (Facultatif) Installez et configurez VMware App Volumes 2.14 ou version ultérieure, qui fournit des fonctionnalités de distribution d'applications en temps réel.

   Reportez-vous au document *Guide d'installation de VMware App Volumes* pour plus d'informations.

5. (Facultatif) Pour fournir une gestion contextuelle des stratégies, installez et configurez VMware Dynamic Environment Manager 9.2.1 ou version ultérieure.

   Reportez-vous au document *Installation et configuration de VMware Dynamic Environment Manager*.

6. Obtenez les certificats SSL signés par une autorité de certification qui doivent être utilisés pour que le JMP Server communique en toute sécurité avec d'autres serveurs dans le réseau de votre organisation.

7 Installez JMP Server et configurez les certificats SSL pour que le JMP Server communique avec les autres serveurs qui sont requis pour les fonctionnalités de JMP Integrated Workflow.

   Pour plus d'informations, reportez-vous au document *Guide d'installation et de configuration de VMware Horizon JMP Server*.

8 Configurez les paramètres JMP pour la première fois. Reportez-vous à la section Configurer les paramètres JMP pour la première fois pour plus d'informations.

Étape suivante

Une fois les tâches précédentes correctement terminées, vous pouvez créer une attribution JMP. Pour plus d'informations, reportez-vous à la section Création d'une attribution JMP.

Administration des paramètres JMP

11

Après l'installation de JMP Server, vous devez configurer les paramètres JMP avec les informations d'identification nécessaires avant de pouvoir créer des attributions JMP et commencer à utiliser les fonctionnalités de JMP Integrated Workflow. Vous pouvez modifier les paramètres JMP initiaux et, le cas échéant, ajouter de nouvelles informations de paramètres.

Ce chapitre contient les rubriques suivantes :

Configurer les paramètres JMP pour la première fois

Avant de pouvoir créer des attributions JMP, vous devez configurer les paramètres JMP à l'aide de la Horizon Console. Vous devez fournir les informations d'identification du domaine Active Directory que vous utilisez pour attribuer des espaces de travail de poste de travail pour des utilisateurs ou un groupe d'utilisateurs. Vous pouvez éventuellement inclure les informations d'identification pour utiliser des AppStacks App Volumes et le partage de configuration Dynamic Environment Manager lors de la création d'attributions JMP.

Conditions préalables

- Vérifiez que VMware HorizonJMP Server a été correctement installé et que vous disposez de son URL. Pour plus d'informations, reportez-vous au document *Guide d'installation et de configuration de VMware Horizon JMP Server*.
- Obtenez les informations d'identification administrateur d'Horizon 7 version 7.5 ou ultérieure que vous prévoyez d'utiliser avec JMP Server.
- Obtenez les informations d'identification Active Directory qui doivent être utilisées avec JMP Server.
- Si vous attribuez des applications à des attributions JMP, assurez-vous que vous disposez de l'URL et des informations d'identification de compte de l'instance de VMware App Volumes Manager à utiliser. Si un équilibrage de charge gère vos instances d'App Volumes Manager que vous prévoyez d'utiliser, obtenez l'URL de l'équilibrage de charge et utilisez-la lorsque vous configurez les informations d'App Volumes Manager.

- Si vous choisissez d'utiliser un partage de configuration VMware Dynamic Environment Manager, obtenez son chemin d'accès UNC et les informations d'identification de compte administrateur nécessaires pour y accéder.

Procédure

1. Dans Horizon Console, cliquez sur **Configuration de JMP**.
2. Entrez les informations de JMP Server.
   a. Dans l'onglet **JMP Server**, cliquez sur **Ajouter le JMP Server**.
   b. Entrez l'URL JMP Server au format `https://jmp.yourcompany.com`.
   c. Cliquez sur **Enregistrer**.

   L'URL de JMP Server est validée. Si vous recevez le message `Le JMP Server est inaccessible`, vérifiez que vous avez entré l'URL correcte, que JMP Server est correctement configuré et que JMP Server est accessible.
3. Entrez les informations de compte du Serveur de connexion Horizon 7 version 7.5 ou ultérieure que vous prévoyez d'utiliser avec JMP Server.
   a. Cliquez sur l'onglet **Horizon 7**.
   b. Si elle n'est pas renseignée automatiquement, entrez la valeur **URL du Serveur de connexion**. Cette URL est la même que celle du Serveur de connexion Horizon 7 auquel la Horizon Console est connectée.
   c. Entrez vos nom d'utilisateur et mot de passe du compte de service Horizon 7.
   d. Dans la zone de texte **Domaine du compte de service**, entrez un nom valide à utiliser avec les attributions JMP que vous créez et appuyez sur **Entrée**.
   e. Cliquez sur **Enregistrer**.
4. Entrez les informations du serveur Active Directory que vous allez utiliser avec les attributions JMP.
   a. Cliquez sur l'onglet **Active Directory**.
   b. Cliquez sur **Nouveau**.
   c. Dans la zone de texte **Nom NETBIOS**, faites votre choix dans la liste de noms de domaine NetBIOS disponibles.

      Les zones de texte Nom de domaine DNS et Contexte sont mises à jour avec les valeurs par défaut.
   d. Vérifiez que la valeur par défaut qui a été ajoutée dans la zone de texte **Nom de domaine DNS** est la valeur correcte à utiliser. Vous pouvez également entrer un autre nom de domaine Active Directory complet. Par exemple, `mycompany.com`.
   e. Dans la section **Protocole**, sélectionnez le protocole utilisé par votre annuaire Active Directory.

f Dans les zones de texte **Nom d'utilisateur de liaison** et **Mot de passe de liaison**, entrez les informations d'identification du compte d'utilisateur Nom unique de liaison. Par exemple, `administrateur`.

g Modifiez la valeur dans la zone de texte **Contexte**, si vous souhaitez utiliser une valeur différente de la valeur par défaut.

La valeur est utilisée en tant que racine pour la recherche de données Active Directory.

h (Facultatif) Cliquez sur **Propriétés avancées** et modifiez la valeur numérique par défaut de Port.

La valeur de Port par défaut est basée sur le protocole que vous avez sélectionné précédemment. Vous pouvez modifier la valeur de Port ou laisser la zone de texte vide.

i Dans la zone de texte **Contrôleur de domaine**, entrez éventuellement un ou plusieurs noms d'hôte ou adresses IP à utiliser pour gérer le trafic Active Directory.

Par exemple, `adserver.mycompany.com, 10.111.XXX.XXX`. Si la zone de texte est vide, la valeur dans la zone de texte **Nom de domaine DNS** est utilisée.

j Cliquez sur **Enregistrer**.

5 Si vous prévoyez d'utiliser des AppStacks App Volumes lors de la création d'attributions JMP, configurez l'instance d'App Volumes Manager que vous prévoyez d'utiliser.

a Cliquez sur l'onglet **App Volumes**.

b Cliquez sur **Nouveau**.

c Dans la zone de texte **Nom**, entrez un nom à attribuer à l'instance d'App Volumes. Si vous laissez la zone de texte vide, la valeur que vous entrez dans la zone de texte **URL d'App Volumes Server** est utilisée.

d Entrez une URL valide pour l'instance d'App Volumes Manager à laquelle vous voulez que l'espace JMP Server soit associé.

Important Si un équilibrage de charge gère l'instance d'App Volumes Manager que vous prévoyez d'utiliser, entrez l'URL de cet équilibrage de charge.

e Entrez les informations d'identification du compte d'administrateur d'App Volumes Manager ou de l'équilibrage de charge que votre JMP Server peut utiliser pour accéder à votre instance d'App Volumes Manager.

f Entrez le nom de domaine pour le compte de service d'App Volumes Manager utilisé pour les attributions JMP.

g (Facultatif) Si vous enregistrez plusieurs instances d'App Volumes Manager, utilisez le bouton bascule pour indiquer si l'instance d'App Volumes Manager que vous ajoutez est le serveur par défaut à utiliser lors de la création d'attributions JMP. Vous pouvez modifier l'instance que vous voulez utiliser lors de la création d'une attribution JMP.

h Cliquez sur **Enregistrer**.

6 Si vous voulez utiliser un partage de configuration Dynamic Environment Manager lorsque vous créez des attributions JMP, ajoutez ses informations aux paramètres JMP.

a Cliquez sur l'onglet **UEM**.

b Cliquez sur **Nouveau**.

c Entrez une valeur dans la zone de texte **Chemin UNC du partage de fichiers** au format `\\nom-serveurfichier\nom-chemin-partage-configuration-UEM`. Par exemple, `\\Serveurfichier\UEMConfig`.

Important N'incluez pas `Général` dans le chemin UNC de partage de fichier que vous entrez.

d Entrez les informations d'identification du compte d'administrateur Dynamic Environment Manager à utiliser pour se connecter au partage de configuration Dynamic Environment Manager.

e Dans la liste **Active Directory**, sélectionnez le nom de domaine à utiliser avec le partage de configuration Dynamic Environment Manager.

Note Un annuaire Active Directory ne peut être associé qu'à un seul partage de configuration Dynamic Environment Manager.

f Cliquez sur **Enregistrer**.

Étape suivante

Après avoir configuré correctement les paramètres JMP initiaux, vous pouvez créer des attributions JMP. Pour plus d'informations, reportez-vous à la section Création d'une attribution JMP.

Gestion des paramètres JMP

Vous pouvez utiliser la Horizon Console pour modifier, ajouter ou supprimer des informations pour un paramètre JMP.

- Vous devez disposer des informations nécessaires pour modifier le paramètre JMP spécifique.
- Pour modifier les paramètres JMP, assurez-vous de disposer des privilèges d'administration appropriés.

Modifier les paramètres JMP Server

Vous pouvez utiliser la Horizon Console pour apporter des modifications aux paramètres JMP Server existants.

Conditions préalables

- Vous devez disposer des informations nécessaires pour modifier les paramètres JMP Server spécifiques.
- Assurez-vous de disposer des privilèges d'administration appropriés pour vous connecter à la Horizon Console et modifier les paramètres JMP Server.

Procédure

1. Dans Horizon Console, sélectionnez **Configuration de JMP**.
2. Dans le volet Paramètres JMP, cliquez sur l'onglet **JMP Server**.
3. Cliquez sur **Modifier**.
4. Entrez une nouvelle **URL de JMP Server**.
5. Cliquez sur **Enregistrer**.

La nouvelle URL de JMP Server est validée et, si elle n'est pas valide, un message d'erreur s'affiche.

Modifier les informations d'identification d'Horizon 7

Utilisez la Horizon Console pour modifier les informations d'identification du Serveur de connexion Horizon 7 existant.

Procédure

1. Dans Horizon Console, cliquez sur **Configuration de JMP**.
2. Cliquez sur l'onglet **Horizon 7**.
3. Cliquez sur **Modifier les informations d'identification**.
4. Entrez un nouveau nom d'utilisateur dans **Nom d'utilisateur du compte de service**, si nécessaire.
5. Entrez un nouveau mot de passe dans **Mot de passe du compte de service**, si nécessaire.
6. Modifiez la valeur dans **Domaine du compte de service**, si nécessaire.
7. Cliquez sur **Enregistrer**.

Modifier l'URL du Serveur de connexion Horizon

Si vous voulez associer des attributions JMP existantes à un autre Horizon Connection Server, vous devez modifier l'URL d'Horizon Connection Server qui est enregistrée avec les paramètres JMP Server associés aux attributions JMP.

Il n'existe aucune interface utilisateur dans la Horizon Console qui vous permet de modifier les informations d'Horizon Connection Server. Vous devez utiliser SQL Server Management Studio pour modifier l'URL d'hôte Horizon Connection Server existante dans les paramètres JMP.

Conditions préalables

- Assurez-vous de disposer des privilèges d'administrateur système appropriés pour vous connecter à une session SQL Server Management Studio et pour accéder à la base de données SQL Server que vous avez créée pour JMP Server.
- Sauvegardez votre base de données SQL Server avant de passer à la modification de la base de données.

Procédure

1. Si vous êtes actuellement connecté à une session Horizon Console, déconnectez-vous.
2. Connectez-vous à une session SQL Server Management Studio en tant que sysadmin (SA) ou en utilisant un compte d'utilisateur avec des privilèges SA.
3. Vérifiez que l'URL d'hôte Horizon Connection Server de remplacement que vous prévoyez d'utiliser n'est pas déjà enregistrée sur une autre instance de JMP Server.

   Par exemple, si l'URL d'hôte Horizon Connection Server de remplacement est `new-horizon-host.com`, utilisez l'instruction SQL suivante pour vérifier qu'elle n'est pas déjà enregistrée.

   ```
   SELECT * from  xms_services
   WHERE xms_services.host = "new-horizon-host.com"
   ```

4. Si l'instruction SQL précédente n'a renvoyé aucun résultat, passez à l'étape suivante. Dans le cas contraire, utilisez l'instruction suivante pour supprimer les informations de l'hôte Horizon Connection Server existant.

   ```
   DELETE from xms_services
   WHERE xms_services.host = "new-horizon-host.com"
   ```

5. Mettez à jour les paramètres JMP Server existants en utilisant les instructions suivantes, où `new-horizon-server-host.com` est l'URL de l'hôte Horizon Connection Server de remplacement et `old-horizon-host.com` est l'URL de l'hôte Horizon Connection Server actuellement enregistré.

   ```
   UPDATE xms_service_endpoints
   SET host = 'new-horizon-host.com', is_available = 1
   WHERE service_id = (SELECT id FROM xms_services WHERE service_type = 'horizon'
       AND host = 'old-horizon-host.com')
   AND host = 'old-horizon-host.com'

   UPDATE xms_services
   SET [name] = 'horizon-https://new-horizon-host.com', host = 'new-horizon-host.com'
   WHERE service_type = 'horizon'
   AND host = 'old-horizon-host.com'
   ```

6. Connectez-vous à la Horizon Console à l'aide de la nouvelle URL Horizon Connection Server et vérifiez que le nouvel hôte Horizon Connection Server est maintenant associé à vos attributions JMP existantes qui étaient précédemment associées à l'ancien hôte Horizon Connection Server.

Ajouter des domaines Active Directory

Si vous devez ajouter un autre domaine Active Directory après la configuration du premier domaine, utilisez la Horizon Console.

Procédure

1. Dans Horizon Console, cliquez sur **Configuration de JMP**.
2. Cliquez sur l'onglet **Active Directory**, puis cliquez sur **Ajouter**.

3 Dans la zone de texte **Nom NETBIOS**, faites votre choix dans la liste de noms de domaine NetBIOS disponibles.

   Les zones de texte Nom de domaine DNS et Contexte sont mises à jour avec les valeurs par défaut.

4 Dans le champ **Nom de domaine DNS**, vérifiez que la valeur par défaut ajoutée après le nom NETBIOS a été mise à jour. Vous pouvez également entrer un autre nom de domaine Active Directory complet. Par exemple, `mycompany.com`.

5 Dans la section **Protocole**, sélectionnez le protocole utilisé par votre annuaire Active Directory.

6 Dans les champs **Nom d'utilisateur de liaison** et **Mot de passe de liaison**, entrez les informations d'identification du compte d'utilisateur Nom unique de liaison, par exemple Administrateur.

7 Modifiez la valeur dans le champ **Contexte**, si vous voulez utiliser une valeur différente de la valeur par défaut.

8 (Facultatif) Cliquez sur **Propriétés avancées** et modifiez la valeur numérique par défaut de Port.

   La valeur de Port par défaut est basée sur le protocole que vous avez sélectionné précédemment. Vous pouvez modifier la valeur de Port ou laisser le champ vide.

9 Dans le champ **Contrôleur de domaine**, entrez éventuellement un ou plusieurs noms d'hôte ou adresses IP à utiliser pour gérer le trafic Active Directory.

10 Cliquez sur **Enregistrer**.

Des informations sur le domaine Active Directory récemment ajouté s'affichent dans le tableau Active Directory.

Modifier des informations sur le domaine Active Directory

Si certaines informations ont été modifiées depuis votre première configuration des paramètres JMP, utilisez la Horizon Console pour modifier les informations de paramètres de domaine Active Directory.

Procédure

1 Dans Horizon Console, cliquez sur **Configuration de JMP**.

2 Cliquez sur l'onglet **Active Directory**.

3 Sélectionnez l'une des lignes dans le tableau des domaines Active Directory et cliquez sur **Modifier**.

4 Modifiez les informations Active Directory qui doivent être mises à jour.

5 Cliquez sur **Enregistrer**.

Supprimer les informations sur le domaine Active Directory

Utilisez Horizon Console si vous devez supprimer des informations existantes dans les paramètres du domaine Active Directory.

Vous ne pouvez supprimer des informations sur un domaine Active Directory enregistré d'un paramètre JMP que si ce domaine n'est pas en cours d'utilisation par des attributions JMP existantes.

Procédure

1. Dans Horizon Console, cliquez sur **Configuration de JMP**.
2. Cliquez sur l'onglet **Active Directory**.
3. Sélectionnez la ligne du tableau du domaine Active Directory que vous voulez supprimer des paramètres JMP.
4. Dans la boîte de dialogue de confirmation de la suppression qui s'affiche, lisez le message et cliquez sur **Supprimer** pour confirmer que vous ne voulez pas supprimer ces informations de domaine Active Directory.

Si aucune attribution JMP n'utilise le domaine Active Directory, il est supprimé.

Si le domaine Active Directory est utilisé par une attribution JMP, une boîte de dialogue d'avertissement s'affiche. Le message d'avertissement comporte la liste d'attributions JMP qui utilisent le domaine Active Directory. Vous pouvez supprimer les informations de domaine après les avoir supprimées des attributions JMP ou après avoir supprimé les attributions JMP qui les utilisent.

Ajouter des informations App Volumes

Utilisez la Horizon Console pour ajouter des informations pour toutes les instances d'App Volumes Manager supplémentaires pouvant être utilisées lors de la création d'attributions JMP.

Procédure

1. Dans Horizon Console, cliquez sur **Configuration de JMP**.
2. Cliquez sur l'onglet **App Volumes**, puis cliquez sur **Ajouter**.

   La boîte de dialogue **Ajouter l'instance d'App Volumes** s'affiche.
3. Dans la zone de texte **Nom**, entrez un nom unique à attribuer à l'instance d'App Volumes. Si vous laissez la zone de texte vide, la valeur que vous entrez dans la zone de texte **URL d'App Volumes Server** est utilisée.
4. Dans la zone de texte **URL d'App Volumes Server**, entrez une URL valide de l'instance d'App Volumes Manager que vous voulez associer à votre instance de JMP Server. Si un équilibrage de charge gère l'instance d'App Volumes Manager que vous ajoutez, entrez l'URL de cet équilibrage de charge.

   Note Si les instances d'App Volumes Manager que vous avez ajoutées sont connectées à différentes bases de données SQL, des informations sur l'instance d'App Volumes Manager que vous ajoutez s'affichent dans l'onglet App Volumes. Si les instances d'App Volumes Manager sont connectées à la même base de données SQL, seules les informations sur l'instance d'App Volumes Manager enregistrée précédemment apparaissent dans l'onglet App Volumes.
5. Entrez le nom d'utilisateur et le mot de passe d'administrateur App Volumes que votre instance de JMP Server peut utiliser pour accéder à votre instance d'App Volumes Manager.
6. Entrez le nom de domaine du compte de service App Volumes utilisé pour les attributions JMP.

7 Pour que l'instance d'App Volumes Manager que vous êtes en train d'ajouter soit le serveur d'App Volumes Manager par défaut utilisé lors de la création d'attributions JMP, cliquez sur le bouton bascule. Vous pouvez modifier le serveur que vous voulez utiliser lors de la création d'une attribution JMP.

   Le bouton bascule devient bleu avec l'étiquette **Oui**.

8 Cliquez sur **Enregistrer**.

Modifier les informations sur l'instance d'App Volumes

Si vous devez modifier les informations existantes sur l'instance d'App Volumes qui est utilisée par les attributions JMP, utilisez la Horizon Console pour modifier les informations.

Procédure

1 Dans Horizon Console, cliquez sur **Configuration de JMP**.

2 Cliquez sur l'onglet **App Volumes** et sélectionnez la ligne du tableau pour l'instance d'App Volumes que vous voulez modifier.

3 Cliquez sur **Modifier**.

   La boîte de dialogue **Ajouter l'instance d'App Volumes** s'affiche.

4 Modifiez les informations sur l'instance d'App Volumes qui doivent être mises à jour.

5 Cliquez sur **Enregistrer**.

Supprimer des informations sur l'instance d'App Volumes

Utilisez la Horizon Console si vous devez supprimer les informations de paramètres existantes sur une instance d'App Volumes.

Vous ne pouvez supprimer des informations sur une instance App Volumes enregistrée d'un paramètre JMP que si cette instance n'est utilisée par aucune attribution JMP.

Procédure

1 Dans Horizon Console, cliquez sur **Configuration de JMP**.

2 Cliquez sur l'onglet **App Volumes**.

3 Sélectionnez la ligne des informations sur l'instance d'App Volumes que vous voulez supprimer des paramètres JMP.

4 Cliquez sur **Supprimer** pour confirmer que vous voulez supprimer ces informations sur l'instance d'App Volumes.

Si aucune attribution JMP n'utilise l'instance d'App Volumes, elle est supprimée.

Si l'instance d'App Volumes est utilisée par une attribution JMP, une boîte de dialogue d'avertissement s'affiche. Le message d'avertissement comporte la liste d'attributions JMP qui utilisent l'instance d'App Volumes. Vous pouvez supprimer les informations sur l'instance d'App Volumes après les avoir supprimées des attributions JMP ou après avoir supprimé les attributions JMP qui les utilisent.

Ajouter des informations de partage de configuration Dynamic Environment Manager

Utilisez la Horizon Console si vous devez ajouter un autre partage de configuration Dynamic Environment Manager après avoir défini le partage initial.

Vous ne pouvez ajouter qu'un seul partage de configuration Dynamic Environment Manager par domaine AD. Par conséquent, le partage de configuration que vous êtes sur le point d'ajouter ne peut pas avoir la même adresse IP ou DNS que les partages de configuration déjà inclus dans les paramètres de votre JMP Server.

Procédure

1. Dans Horizon Console, cliquez sur **Configuration de JMP**.
2. Cliquez sur l'onglet **UEM** et sur **Ajouter**.

   La boîte de dialogue **Ajouter un partage de fichiers UEM** s'affiche.
3. Entrez une valeur dans la zone de texte **Chemin UNC du partage de fichiers** au format `\\`*`nom-serveur\nom-chemin-partage-configuration-UEM`*.

   Par exemple, si l'emplacement du partage de configuration est `\\<adresse-IP>\uemshare\config \general\FlexRepository\..`, le chemin d'accès que vous devez entrer dans la zone de texte **Chemin UNC du partage de fichiers** est **`\\<adresse-IP>\uemshare\config`**.
4. Entrez le nom d'utilisateur et le mot de passe d'Dynamic Environment Manager qui doivent être utilisés pour se connecter au partage de fichiers de configuration Dynamic Environment Manager.
5. Dans la liste **Active Directory**, sélectionnez le nom de domaine à utiliser avec le partage de fichiers de configuration Dynamic Environment Manager.

   Note Un annuaire Active Directory ne peut être associé qu'à un seul partage de fichiers de configuration Dynamic Environment Manager.
6. Cliquez sur **Enregistrer**.

Les informations sur le partage de fichiers de configuration Dynamic Environment Manager sont ajoutées aux paramètres JMP et une nouvelle ligne est ajoutée au tableau dans l'onglet **UEM**.

Modifier les informations sur le partage de fichiers de configuration Dynamic Environment Manager

Utilisez la Horizon Console si vous devez modifier les informations existantes sur le partage de fichiers de configuration Dynamic Environment Manager qui est utilisé par les attributions JMP.

Procédure

1. Dans Horizon Console, cliquez sur **Configuration de JMP**.
2. Cliquez sur l'onglet **UEM** et, à partir du tableau des informations existantes, sélectionnez la ligne du partage de fichiers de configuration Dynamic Environment Manager que vous voulez modifier.
3. Cliquez sur **Modifier**.

   La boîte de dialogue **Modifier le partage de fichiers UEM** s'affiche.
4. Modifiez les informations sur le partage de fichiers de configuration Dynamic Environment Manager qui doivent être mises à jour.
5. Cliquez sur **Enregistrer**.

Supprimer des informations de partage de configuration Dynamic Environment Manager

Utilisez la Horizon Console si vous devez supprimer les informations de paramètres existantes sur un partage de configuration Dynamic Environment Manager.

Vous ne pouvez supprimer des informations sur un partage de configuration Dynamic Environment Manager enregistré d'un paramètre JMP que si ce partage de configuration n'est utilisé par aucune attribution JMP.

Procédure

1. Dans Horizon Console, cliquez sur **Configuration de JMP**.
2. Cliquez sur l'onglet **UEM**.
3. Sélectionnez la ligne des informations sur le partage de configuration Dynamic Environment Manager que vous voulez supprimer des paramètres JMP.
4. Cliquez sur **Supprimer** pour confirmer que vous voulez supprimer ces informations sur le partage de configuration Dynamic Environment Manager.

Si aucune attribution JMP n'utilise le partage de configuration Dynamic Environment Manager, il est supprimé.

Si le partage de configuration Dynamic Environment Manager est utilisé par une attribution JMP, une boîte de dialogue d'avertissement s'affiche. Le message d'avertissement comporte la liste d'attributions JMP qui utilisent le partage de configuration Dynamic Environment Manager. Vous pouvez supprimer les informations sur le partage de configuration Dynamic Environment Manager après les avoir supprimées des attributions JMP ou après avoir supprimé les attributions JMP qui les utilisent.

Administration des attributions JMP

12

Après avoir installé JMP Server et configuré les paramètres JMP, vous pouvez commencer à utiliser les fonctionnalités de JMP Integrated Workflow pour créer, modifier, dupliquer ou supprimer des attributions JMP.

Vous devez tout d'abord installer JMP Server et configurer les paramètres JMP avant de pouvoir créer des attributions JMP. Pour plus d'informations, reportez-vous au *Guide d'installation et de configuration de VMware Horizon JMP Server* et à la section Configurer les paramètres JMP pour la première fois.

Vérifiez que les conditions préalables suivantes sont réunies avant de créer, modifier, dupliquer ou supprimer des attributions JMP.

- Vérifiez que l'instance d'Horizon 7 qui est enregistrée avec le paramètre JMP est en cours d'exécution.
- Assurez-vous qu'il existe au moins un domaine Active Directory enregistré avec le paramètre JMP.
- Vérifiez que l'instance d'App Volumes que vous avez enregistrée avec le paramètre JMP est en cours d'exécution.
- Vérifiez que le partage de configuration d'Dynamic Environment Manager défini dans le paramètre JMP est en cours d'exécution.

Note Les droits d'accès globaux ne sont pas pris en charge.

Lorsque vous tentez de créer, modifier, dupliquer ou supprimer une attribution JMP, vous pouvez recevoir un message indiquant que l'action tentée ne s'est pas terminée correctement. Par exemple, certains problèmes peuvent se produire lorsque vous tentez d'atteindre l'un des composants de technologie JMP sous-jacents et la validation des attributions ne se termine pas correctement. Sur l'écran de résumé Attribution JMP, vous pouvez essayer de corriger le problème en sélectionnant l'une des options suivantes.

- Cliquez sur **Modifier** pour corriger les problèmes manuellement.
- Cliquez sur **Réparer** pour que le JMP Server tente de résoudre les problèmes détectés sur l'attribution JMP actuelle.
- Cliquez sur **Forcer la suppression** pour supprimer complètement l'attribution JMP.

Ce chapitre contient les rubriques suivantes :

- Modification d'une attribution JMP
- Duplication d'une attribution JMP
- Suppression d'une attribution JMP

Création d'une attribution JMP

À l'aide de la Horizon Console, vous pouvez créer des attributions JMP, que vous utilisez pour créer des espaces de travail de poste de travail pour des utilisateurs ou un groupe d'utilisateurs.

Vous sélectionnez les pools de postes de travail Horizon, les AppStacks d'App Volumes et les paramètres d'User Environment Manager pour définir une attribution JMP.

Conditions préalables

Vérifiez que les conditions préalables répertoriées dans la section Chapitre 12 Administration des attributions JMP ont été remplies.

Procédure

1. Dans Horizon Console, cliquez sur **Attributions (JMP)**.
2. Cliquez sur **Nouveau**.
3. Dans l'onglet **Utilisateurs** de l'assistant Nouvelle attribution, entrez quelques caractères en regard de la liste déroulante Active Directory et sélectionnez les utilisateurs ou un groupe d'utilisateurs à inclure dans la nouvelle attribution JMP.

   Votre sélection est ajoutée dans la section Utilisateurs/groupes sélectionnés.
4. Cliquez sur **Suivant**.
5. Dans l'onglet **Postes de travail**, sélectionnez le pool de postes de travail à inclure dans l'attribution JMP et cliquez sur **Suivant**.
6. Dans l'onglet **Applications**, cliquez sur la case à cocher en regard du nom de l'application que vous souhaitez inclure dans l'attribution JMP. Lorsque vous avez terminé avec votre sélection, cliquez sur **Suivant**.
7. Dans l'onglet **Environnement utilisateur**, décidez si vous voulez configurer l'attribution JMP avec les paramètres d'environnement utilisateur disponibles.
   - Avec **Désactiver les paramètres UEM ?** défini sur **Non**, le fait de cliquer sur **Ignorer** signifie que le fichier d'attribution d'User Environment Manager ne va pas être enregistré dans le partage de configuration d'User Environment Manager. Tous les paramètres d'User Environment Manager vont être appliqués aux espaces de travail de poste de travail virtuel créés pour les utilisateurs utilisant l'attribution JMP que vous créez.
   - Avec **Désactiver les paramètres UEM ?** défini sur **Non**, sélectionnez les paramètres d'environnement utilisateur que vous voulez appliquer à l'attribution JMP en cours de création. Le

fait de cliquer sur **Suivant** crée le fichier d'attribution d'User Environment Manager avec les paramètres d'environnement utilisateur sélectionnés. Les paramètres sélectionnés sont appliqués aux espaces de travail de poste de travail virtuel créés pour les utilisateurs utilisant l'attribution JMP que vous créez.

- Avec **Désactiver les paramètres UEM ?** défini sur **Oui**, la liste des paramètres d'environnement utilisateur disponibles sont supprimés de la vue. Lorsque vous cliquez sur **Suivant**, un fichier d'attribution vide est consigné dans le partage de configuration d'User Environment Manager. Le fait de désactiver les paramètres d'User Environment Manager garantit qu'aucun paramètre d'environnement utilisateur n'est appliqué aux espaces de travail de poste de travail virtuel créés pour les utilisateurs utilisant l'attribution JMP que vous créez.

8. Dans l'onglet **Définitions**, acceptez le nom par défaut pour l'attribution JMP ou remplacez le nom par un autre et ajoutez éventuellement une description.
9. Dans la liste déroulante **Liaison d'AppStack**, sélectionnez le moment auquel l'AppStack doit être associée à l'attribution JMP, puis cliquez sur **Suivant**.
10. Dans l'onglet **Résumé**, examinez les détails de la nouvelle attribution. S'ils sont acceptables, cliquez sur **Envoyer**. Si des modifications doivent être effectuées, cliquez sur **Précédent** pour faire les changements.

La nouvelle attribution JMP est mise en attente pour le stockage dans la base de données JMP et est ajoutée à la liste d'attributions dans le volet Attributions JMP. Une fois que l'attribution JMP est ajoutée à la base de données JMP, l'état quitte l'état En attente. Elle devient sélectionnable dans la liste d'attributions JMP et vous pouvez la modifier, la dupliquer ou la supprimer.

Vous pouvez également vérifier les attributions ou les droits d'accès qui ont été créés pour la nouvelle attribution JMP en utilisant les informations suivantes.

- Pour vérifier les informations sur le pool de postes de travail Horizon créé pour l'attribution JMP, utilisez Horizon Console. Sélectionnez **Inventaire > Postes de travail** et localisez le pool de postes de travail créé par JMP Server.
- Pour afficher les informations sur les AppStacks créés par JMP Server de la nouvelle attribution JMP, utilisez la console d'App Volumes Manager. Sélectionnez **Volumes > AppStacks** et localisez les AppStacks créés par JMP Server.
- Pour vérifier les paramètres d'environnement utilisateur que vous avez configurés pour l'attribution JMP, utilisez la console de gestion Dynamic Environment Manager et cliquez sur l'onglet **Environnement utilisateur**. Dans le volet de gauche, sélectionnez le paramètre d'environnement utilisateur utilisé par l'attribution JMP et cliquez sur l'onglet **Attributions** de la boîte de dialogue qui s'ouvre pour afficher les informations relatives à l'attribution JMP pour ce paramètre d'environnement utilisateur.

Modification d'une attribution JMP

Vous devrez peut-être modifier une attribution JMP existante en raison des modifications apportées aux composants qui ont été utilisés pour la définir. Vous pouvez utiliser Horizon Console pour apporter les modifications nécessaires à l'attribution JMP.

Conditions préalables

- Vérifiez que les conditions préalables répertoriées dans la section Chapitre 12 Administration des attributions JMP ont été remplies.
- L'état de l'attribution JMP que vous prévoyez de modifier ne doit pas être « En attente ».

Procédure

1. Dans Horizon Console, cliquez sur **Attributions (JMP)**.
2. Sélectionnez l'attribution JMP à modifier en cliquant sur la case à cocher ou sur le nom de l'attribution JMP dans la liste.
3. Cliquez sur **Modifier**.
4. Dans l'assistant Modifier l'attribution, modifiez les paramètres actuels.

   Cliquez sur **Annuler** si vous voulez interrompre à tout moment le processus de modification.

   a. Si vous voulez supprimer l'un des utilisateurs ou des groupes actuellement sélectionnés, cliquez sur l'icône Supprimer (**X**).

   b. Cliquez sur **Suivant**.

   c. Dans l'onglet **Postes de travail**, sélectionnez un pool de postes de travail que vous voulez inclure dans l'attribution JMP. Cliquez sur **Suivant**.

   d. Dans l'onglet **Applications**, sélectionnez les applications disponibles que vous voulez ajouter à l'attribution JMP ou désélectionnez celles qui ont été précédemment sélectionnées. Cliquez sur **Suivant**.

e Dans l'onglet **Environnement utilisateur**, décidez si vous voulez configurer l'attribution JMP avec les paramètres d'environnement utilisateur disponibles.

- Avec **Désactiver les paramètres UEM ?** défini sur **Non**, le fait de cliquer sur **Ignorer** signifie que le fichier d'attribution d'User Environment Manager ne va pas être enregistré dans le partage de configuration d'User Environment Manager. Tous les paramètres d'User Environment Manager vont être appliqués aux espaces de travail de poste de travail virtuel créés pour les utilisateurs utilisant l'attribution JMP que vous modifiez.
- Avec **Désactiver les paramètres UEM ?** défini sur **Non**, sélectionnez les paramètres d'environnement utilisateur que vous voulez appliquer à l'attribution JMP en cours de création. Le fait de cliquer sur **Suivant** crée le fichier d'attribution d'User Environment Manager avec les paramètres d'environnement utilisateur sélectionnés. Les paramètres sélectionnés sont appliqués aux espaces de travail de poste de travail virtuel créés pour les utilisateurs utilisant l'attribution JMP que vous modifiez.
- Avec **Désactiver les paramètres UEM ?** défini sur **Oui**, la liste des paramètres d'environnement utilisateur disponibles sont supprimés de la vue. Lorsque vous cliquez sur **Suivant**, un fichier d'attribution vide est consigné dans le partage de configuration d'User Environment Manager. Le fait de désactiver les paramètres d'User Environment Manager garantit qu'aucun paramètre d'environnement utilisateur n'est appliqué aux espaces de travail de poste de travail virtuel créés pour les utilisateurs utilisant l'attribution JMP que vous modifiez.

f Dans l'onglet **Définitions**, le cas échéant, modifiez les valeurs actuelles de **Nom**, **Description** ou l'heure à laquelle vous voulez lier l'AppStack à l'attribution JMP.

g Cliquez sur **Suivant**.

h Examinez le résumé des modifications que vous avez apportées et cliquez sur **Envoyer** pour enregistrer les modifications.

Si l'opération réussit, les modifications sont enregistrées. Si des problèmes sont rencontrés, des informations supplémentaires sont fournies et les actions possibles que vous pouvez prendre s'affichent.

Duplication d'une attribution JMP

Vous pouvez créer des attributions JMP plus rapidement en dupliquant des attributions JMP existantes qui sont semblables à celles que vous voulez créer.

Conditions préalables

- Vérifiez que les conditions préalables répertoriées dans la section Chapitre 12 Administration des attributions JMP ont été remplies.
- L'état de l'attribution JMP que vous prévoyez de dupliquer ne doit pas être « En attente » ou « Erreur ».

Procédure

1. Dans Horizon Console, sélectionnez **Attributions (JMP)**.
2. Sélectionnez l'attribution JMP que vous voulez dupliquer et cliquez sur **Dupliquer**.
3. Dans l'assistant Nouvelle attribution, modifiez l'attribution JMP dupliquée si nécessaire.
   a. Sélectionnez de nouveaux utilisateurs ou groupes ou supprimez l'un des utilisateurs ou des groupes actuellement sélectionnés. Cliquez sur **Suivant**.
   b. Dans le volet Postes de travail, sélectionnez un nouveau pool de postes de travail ou supprimez l'un des pools de postes de travail qui était inclus dans l'attribution JMP en double. Cliquez sur **Suivant**.
   c. Sélectionnez des applications supplémentaires à inclure dans la nouvelle attribution JMP et décochez la case de celles actuellement sélectionnées. Cliquez sur **Suivant**.
   d. Dans le volet Environnement utilisateur, sélectionnez le paramètre User Environment Manager que vous voulez appliquer à la nouvelle attribution JMP. Cliquez sur **Suivant**.
   e. Dans le volet Définitions, remplacez le nom par défaut créé, si vous le désirez. Ajoutez une description et spécifiez quand vous voulez que l'AppStack soit lié à la nouvelle attribution JMP.
   f. Cliquez sur **Suivant** et examinez le résumé des détails de la nouvelle attribution JMP.
   g. Si les informations sont satisfaisantes, cliquez sur **Envoyer**. Dans le cas contraire, cliquez sur **Précédent** pour apporter des corrections.

La nouvelle attribution JMP est validée, ce qui peut prendre un certain temps. Une fois validée, l'attribution JMP récemment créée est ajoutée à la liste dans le volet Attributions JMP. Lorsque vous passez le curseur sur son nom, vous constatez que son état est en attente tant qu'elle n'est pas enregistrée correctement dans la base de données JMP. Lorsque l'état de l'attribution JMP n'est plus en attente, vous pouvez effectuer des actions supplémentaires sur l'attribution.

Suppression d'une attribution JMP

Utilisez la Horizon Console pour supprimer une attribution JMP.

Lorsqu'une attribution JMP est supprimée, le droit du pool Horizon, l'attribution d'AppStack et le droit UEM associé à l'attribution JMP sont supprimés. Toutefois, si l'attribution d'AppStack ou le droit du pool Horizon utilisé par l'attribution JMP existait avant la création de l'attribution JMP, ils ne sont pas supprimés. Après la suppression d'une attribution JMP, elle ne s'applique plus à des utilisateurs ou à des postes de travail.

Conditions préalables

- Vérifiez que les conditions préalables répertoriées dans la section Chapitre 12 Administration des attributions JMP ont été remplies.
- L'état de l'attribution JMP que vous prévoyez de supprimer ne doit pas être « En attente ».

Procédure

1. Dans la Horizon Console, cliquez sur **Attributions (JMP)**.
2. Dans le volet Attributions JMP, sélectionnez une ou plusieurs attributions JMP et cliquez sur **Supprimer**.
3. Dans la boîte de dialogue de confirmation, cliquez sur **Supprimer** pour confirmer que vous voulez supprimer définitivement l'attribution.

Si l'opération réussit, le droit du pool Horizon est supprimé de la base de données JMP et de la liste dans le volet Attributions JMP.

Si une partie de l'opération de suppression échoue, l'attribution JMP n'est pas supprimée. Cliquez sur les indicateurs d'état pour voir plus d'informations sur la raison de l'échec de l'opération de suppression.

Configuration des rapports d'événements dans Horizon Console

13

Vous pouvez créer une base de données des événements pour enregistrer des informations sur des événements d'Horizon 7. En outre, si vous utilisez un serveur Syslog, vous pouvez configurer le Serveur de connexion pour qu'il envoie des événements à un serveur Syslog ou créer un fichier plat d'événements écrit au format `Syslog`.

Ce chapitre contient les rubriques suivantes :

Ajouter une base de données et un utilisateur de base de données pour des événements Horizon 7 dans Horizon Console

Vous créez une base de données des événements en l'ajoutant à un serveur de base de données existant. Vous pouvez alors utiliser un logiciel de reporting pour analyser les événements dans la base de données.

Déployez le serveur de base de données pour la base de données d'événements sur un serveur dédié, afin que l'activité de journalisation d'événements n'ait pas d'incidence sur le provisionnement et les autres activités critiques pour les déploiements de Horizon 7.

Note Vous n'avez pas à créer une source de données ODBC pour cette base de données.

Conditions préalables

- Vérifiez que vous possédez un serveur de base de données Microsoft SQL Server ou Oracle pris en charge sur un système auquel une instance du Serveur de connexion a accès.

Pour obtenir les informations les plus récentes sur les bases de données prises en charge, reportez-vous aux matrices d'interopérabilité des produits VMware à l'adresse http://www.vmware.com/resources/compatibility/sim/interop_matrix.php. Pour en savoir plus sur l'**interopérabilité entre les solutions et les bases de données**, après avoir sélectionné le produit et la version, à l'étape Ajouter une base de données, pour afficher une liste de toutes les bases de données prises en charge, sélectionnez **Toutes** et cliquez sur **Ajouter**.

- Vérifiez que vous disposez des privilèges de base de données requis pour créer une base de données et un utilisateur sur le serveur de base de données.
- Si vous n'êtes pas familiarisé avec la procédure de création de bases de données sur des serveurs de base de données Microsoft SQL Server, reportez-vous à la section « Ajouter une base de données View Composer à SQL Server » dans le document *Installation d'Horizon 7*.
- Si vous n'êtes pas familiarisé avec la procédure de création de bases de données sur des serveurs de base de données Oracle, reportez-vous à la section « Ajouter une base de données View Composer à Oracle 12c ou 11g » dans le document *Installation d'Horizon 7*.

Procédure

1. Ajoutez une base de données au serveur et donnez-lui un nom descriptif tel que HorizonEvents.

   Pour une base de données Oracle 12c ou Oracle 11g, fournissez également un préfixe d'Identificateur système Oracle (SID) que vous utilisez lorsque vous configurez la base de données des événements dans Horizon Console.

2. Ajoutez un utilisateur à cette base de données qui a l'autorisation de créer des tableaux, des vues, des déclenchements et des séquences Oracle, ainsi que l'autorisation de lire ces objets et d'écrire sur ces objets.

   Pour une base de données Microsoft SQL Server, n'utilisez pas la méthode du modèle de sécurité d'authentification Windows intégrée. Vérifiez que vous utilisez la méthode d'authentification de SQL Server.

La base de données est créée, mais le schéma n'est pas installé tant que vous n'avez pas configuré la base de données dans Horizon Console.

Étape suivante

Suivez les instructions de la section Configurer la base de données des événements dans Horizon Console.

Préparer une base de données SQL Server pour le reporting d'événements dans Horizon Console

Avant de pouvoir utiliser Horizon Console pour configurer une base de données des événements sur Microsoft SQL Server, vous devez configurer les propriétés TCP/IP correctes et vérifier que le serveur utilise l'authentification SQL Server.

Conditions préalables

- Créez une base de données SQL Server pour le reporting d'événements. Reportez-vous à la section Ajouter une base de données et un utilisateur de base de données pour des événements Horizon 7 dans Horizon Console.
- Vérifiez que vous disposez des privilèges de base de données requis pour configurer la base de données.
- Vérifiez que le serveur de base de données utilise la méthode d'authentification SQL Server. N'utilisez pas l'authentification Windows.

Procédure

1. Ouvrez le Gestionnaire de configuration SQL Server et développez **Configuration du réseau SQL Server *YYYY***.
2. Sélectionnez **Protocoles pour *server_name***.
3. Dans la liste de protocoles, cliquez avec le bouton droit sur **TCP/IP** et sélectionnez **Propriétés**.
4. Définissez la propriété **Activé** sur **Oui**.
5. Vérifiez qu'un port est affecté ou, si nécessaire, affectez-en un.

   Pour plus d'informations sur les ports statiques et dynamiques et comment les affecter, consultez l'aide en ligne du Gestionnaire de configuration SQL Server.
6. Vérifiez que ce port n'est pas bloqué par un pare-feu.

Étape suivante

Utilisez Horizon Console pour connecter la base de données au Serveur de connexion. Suivez les instructions de la section Configurer la base de données des événements dans Horizon Console.

Configurer la base de données des événements dans Horizon Console

La base de données des événements stocke des informations sur des événements Horizon 7 sous forme d'enregistrements dans une base de données plutôt que dans un fichier journal.

Vous configurez une base de données des événements après l'installation d'une instance du Serveur de connexion. Vous devez configurer uniquement un hôte dans un groupe du Serveur de connexion. Les hôtes restant dans le groupe sont configurés automatiquement.

Note La sécurité de la connexion de la base de données entre l'instance du Serveur de connexion et une base de données externe est de la responsabilité de l'administrateur, même si le trafic des événements est limité à des informations sur l'intégrité de l'environnement Horizon 7. Si vous voulez prendre des précautions supplémentaires, vous pouvez sécuriser ce canal via IPSec ou d'autres moyens ou vous pouvez déployer la base de données localement sur l'ordinateur Serveur de connexion.

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 d'Horizon 7*.

Vous pouvez également générer des événements Horizon 7 au format `Syslog` pour qu'un logiciel d'analyse tiers puisse accéder aux données d'événement. Vous utilisez la commande `vdmadmin` avec l'option `-I` pour enregistrer les messages d'événements d'Horizon 7 au format `Syslog` dans les fichiers journaux des événements. Reportez-vous à la section « Génération de messages de journal des événements Horizon 7 au format Syslog à l'aide de l'option I » dans le document *Administration d'Horizon 7*.

Conditions préalables

Vous avez besoin des informations suivantes pour configurer une base de données des événements :

- Le nom DNS ou l'adresse IP du serveur de base de données.
- Le type de serveur de base de données : Microsoft SQL Server ou Oracle.
- Le numéro de port utilisé pour accéder au serveur de base de données. Le port par défaut est 1521 pour Oracle et 1433 pour SQL Server. Pour SQL Server, si le serveur de base de données est une instance nommée, ou si vous utilisez SQL Server Express, vous devez déterminer le numéro de port. Pour plus d'informations sur la connexion à une instance nommée de SQL Server, consultez l'article de la Base de connaissances Microsoft à l'adresse http://support.microsoft.com/kb/265808.
- Le nom de la base de données des événements que vous avez créé sur le serveur de base de données. Reportez-vous à la section Ajouter une base de données et un utilisateur de base de données pour des événements Horizon 7 dans Horizon Console.

  Pour une base de données Oracle 12c ou 11g, vous devez utiliser l'Identificateur du système Oracle (SID) comme nom de base de données lorsque vous configurez la base de données des événements dans Horizon Console.
- Le nom d'utilisateur et le mot de passe de l'utilisateur que vous avez créés pour cette base de données. Reportez-vous à la section Ajouter une base de données et un utilisateur de base de données pour des événements Horizon 7 dans Horizon Console.

  Utilisez l'authentification SQL Server pour cet utilisateur. N'utilisez pas la méthode du modèle de sécurité d'authentification Windows intégrée.
- Un préfixe pour les tableaux dans la base de données des événements, par exemple, VE_. Le préfixe permet de partager la base de données sur plusieurs installations d'Horizon 7.

  Note Vous devez saisir des caractères valides pour le logiciel de base de données que vous utilisez. La syntaxe du préfixe n'est pas vérifiée lorsque vous remplissez la boîte de dialogue. Si vous saisissez des caractères qui ne sont pas valides pour le logiciel de base de données que vous utilisez, une erreur se produit lorsque le Serveur de connexion tente de se connecter au serveur de base de données. Le fichier journal indique toutes les erreurs, y compris cette erreur et les autres renvoyées à partir du serveur de base de données si le nom de la base de données n'est pas valide.

Procédure

1. Dans Horizon Console, sélectionnez **Paramètres > Configuration d'événements**.
2. Dans la fenêtre **Base de données des événements**, cliquez sur **Modifier**, saisissez les informations dans les champs fournis et cliquez sur **OK**.

   Pour effacer les informations de la base de données des événements, cliquez sur **Effacer**.
3. (Facultatif) Dans la fenêtre Paramètres des événements, cliquez sur **Modifier**, modifiez le délai d'affichage des événements et le nombre de jours pour classer des événements comme nouveaux et cliquez sur **OK**.

   Ces paramètres concernent la durée pendant laquelle les événements sont répertoriés dans l'interface d'Horizon Console. Après cette durée, les événements ne sont disponibles que dans les tableaux de base de données historiques.
4. Sélectionnez **Contrôle > Événements** pour vérifier que la connexion à la base de données des événements est établie.

   Si la connexion échoue, un message d'erreur apparaît. Si vous utilisez SQL Express ou une instance nommée de SQL Server, vous devez déterminer le numéro de port correct, comme indiqué dans les conditions préalables.

Configurer la journalisation des événements dans un fichier ou un serveur Syslog dans Horizon Console

Vous pouvez générer des événements Horizon 7 au format `Syslog` pour qu'un logiciel d'analyse puisse accéder aux données d'événement.

Vous devez configurer uniquement un hôte dans un groupe du Serveur de connexion. Les hôtes restant dans le groupe sont configurés automatiquement.

Si vous activez la journalisation d'événements basée sur des fichiers, les événements sont accumulés dans un fichier journal local. Si vous spécifiez un partage de fichiers, ces fichiers journaux sont déplacés dans ce partage.

- La taille maximale du répertoire local pour les journaux des événements, y compris les fichiers journaux fermés, avant que les fichiers les plus anciens soient supprimés, est de 300 Mo. La destination par défaut de la sortie Syslog est `%PROGRAMDATA%\VMware\VDM\events\`.
- Utilisez un chemin d'accès UNC pour enregistrer les fichiers journaux afin de conserver longtemps les événements, ou si vous ne possédez pas de serveur Syslog ou de base de données des événements, ou si votre serveur Syslog actuel ne répond pas à vos besoins.

Vous pouvez également utiliser une commande `vdmadmin` pour configurer la journalisation d'événements basée sur des fichiers au format Syslog. Consultez la rubrique sur la génération de messages de journal des événements Horizon 7 au format Syslog à l'aide de l'option `-I` de la commande `vdmadmin`, dans le document *Administration d'Horizon 7*.

Important Lors de l'envoi à un serveur Syslog, des données Syslog sont envoyées sur le réseau sans chiffrement logiciel et elles peuvent contenir des données sensibles, comme des noms d'utilisateur. VMware recommande d'utiliser une sécurité de couche de liaison, telle qu'IPSEC, pour éviter que ces données soient surveillées sur le réseau.

Conditions préalables

Vous avez besoin des informations suivantes pour configurer le Serveur de connexion pour que les événements puissent être enregistrés au format Syslog ou envoyés à un serveur Syslog, ou les deux :

- Si vous prévoyez d'utiliser un serveur Syslog pour écouter les événements Horizon 7 sur un port UDP, vous devez posséder le nom DNS ou l'adresse IP du serveur Syslog et le numéro de port UDP. Le numéro de port UDP par défaut est 514.
- Si vous prévoyez de collecter des journaux dans un format de fichier plat, vous devez posséder le chemin d'accès UNC vers le partage de fichiers et le dossier dans lequel seront stockés les fichiers journaux, et vous devez posséder le nom d'utilisateur, le nom de domaine et le mot de passe d'un compte avec l'autorisation d'écrire sur le partage de fichiers.

Procédure

1. Dans Horizon Console, sélectionnez **Paramètres > Configuration d'événements**.
2. (Facultatif) Dans la zone **Syslog**, pour configurer le Serveur de connexion afin qu'il envoie des événements à un serveur Syslog, cliquez sur **Ajouter** sous **Envoyer à des serveurs Syslog** et indiquez le nom de serveur ou l'adresse IP et le numéro de port UDP.
3. (Facultatif) Dans la zone **Événements dans le système de fichiers**, choisissez s'il convient ou non d'autoriser la génération et le stockage des messages de journal des événements au format Syslog dans des fichiers journaux.

Option	Description
Always	Toujours générer et stocker les messages de journal des événements au format Syslog dans des fichiers journaux.
Enregistrer dans un fichier en cas d'erreur (valeur par défaut)	Enregistrer les événements d'audit dans un fichier journal en cas de problème d'écriture des événements dans la base de données des événements ou sur le serveur Syslog. Cette option est activée par défaut.
Jamais	Ne jamais générer et stocker les messages de journal des événements au format Syslog dans des fichiers journaux.

Les fichiers journaux sont conservés localement, sauf si vous spécifiez un chemin d'accès UNC vers un partage de fichiers.

4 (Facultatif) Pour stocker les messages de journal des événements Horizon 7 sur un partage de fichiers, cliquez sur **Ajouter** sous **Copier vers l'emplacement** et indiquez le chemin d'accès UNC vers le partage de fichiers et le dossier dans lequel seront stockés les fichiers journaux, avec le nom d'utilisateur, le nom de domaine et le mot de passe d'un compte avec l'autorisation d'écrire sur le partage de fichiers.

   Voici un exemple de chemin d'accès UNC :

```
\\syslog-server\folder\file
```

Surveiller les événements dans Horizon 7

La base de données des événements stocke des informations sur les événements qui surviennent sur l'hôte ou le groupe Serveur de connexion, Horizon Agent et Horizon Console, et vous informe du nombre d'événements dans le tableau de bord. Vous pouvez examiner les événements en détail sur la page **Événements**.

Note Les événements sont répertoriés dans l'interface d'Horizon Console 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 d'Horizon 7*.

Note Si la base de données des événements est indisponible, Horizon 7 conserve la piste d'audit des événements qui se produisent pendant cette période d'indisponibilité et les enregistre dans la base de données des événements dès qu'elle devient disponible. Vous devez redémarrer la base de données des événements et le Serveur de connexion pour afficher ces événements dans l'interface d'Horizon Console.

Vous pouvez non seulement surveiller les événements dans Horizon Console, mais également générer des événements Horizon 7 au format `Syslog` pour qu'un logiciel d'analyse puisse accéder aux données des événements. Reportez-vous aux sections Configurer la journalisation des événements dans un fichier ou un serveur Syslog dans Horizon Console et « Génération de messages de journal des événements Horizon 7 au format Syslog à l'aide de l'option l » dans le document *Installation d'Horizon 7*.

Si vous configurez une base de données des événements pour plusieurs Serveurs de connexion, Horizon Console affiche les événements de tous les Serveurs de connexion sur la page **Événements**. Horizon Console filtre les événements en fonction des tâches que vous effectuez et affiche ces événements sur les pages pertinentes, telles que les pages **Pools de postes de travail** ou **Pools d'applications**.

Conditions préalables

Créez et configurez la base de données des événements comme décrit dans le document *Installation d'Horizon 7*.

Procédure

1 Dans Horizon Console, sélectionnez **Surveiller > Événements**.

2 (Facultatif) Sur la page **Événements**, vous pouvez sélectionner la période des événements, appliquer des filtres aux événements et trier les événements répertoriés sur une ou plusieurs colonnes.

Étape suivante

Dans Horizon Console, accédez à un pool de postes de travail ou d'applications, une machine virtuelle, un disque persistant ou un utilisateur ou un groupe, puis cliquez sur l'onglet **Événements** pour afficher des événements spécifiques.

Messages d'événements Horizon 7

Horizon 7 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.

Le tableau suivant présente les types d'événements signalés par Horizon 7.

Tableau 13-1. Types d'événements signalés par Horizon 7

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 Horizon 7.
Erreur	Signale l'échec d'une opération effectuée par Horizon 7.
Informations	Signale des opérations normales dans Horizon 7.
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.

Utilisation d'Horizon Help Desk Tool dans la Horizon Console

14

Horizon Help Desk Tool est une application Web que vous pouvez utiliser pour obtenir l'état des sessions utilisateur Horizon 7 et effectuer des opérations de dépannage et de maintenance.

Dans Horizon Help Desk Tool, vous pouvez rechercher des sessions utilisateur pour résoudre des problèmes et exécuter des opérations de maintenance de poste de travail, telles que redémarrer ou réinitialiser des postes de travail.

Pour configurer Horizon Help Desk Tool, vous devez respecter les exigences suivantes :

- Licence d'édition d'Horizon Enterprise ou licence d'édition avancée d'Horizon Apps pour Horizon 7. Pour vérifier que vous disposez de la licence correcte, consultez le document *Administration d'Horizon 7*.
- Base de données d'événements pour stocker des informations sur les composants Horizon 7. Pour plus d'informations sur la configuration d'une base de données d'événements, reportez-vous au document *Administration d'Horizon 7*.
- Rôle Administrateur du service d'assistance ou rôle Administrateur du service d'assistance (lecture seule) pour se connecter à Horizon Help Desk Tool. Pour plus d'informations sur ces rôles, reportez-vous au document *Administration d'Horizon 7*.
- Activez le profileur de minutage sur chaque instance du Serveur de connexion pour afficher les segments d'ouverture de session.

  Pour ce faire, utilisez la commande `vdmadmin` suivante :

  ```
  vdmadmin -I -timingProfiler -enable
  ```

  Utilisez la commande `vdmadmin` suivante pour activer le profileur de minutage sur une instance du Serveur de connexion qui utilise un port de gestion :

  ```
  vdmadmin -I -timingProfiler -enable -server {ip/server}
  ```

Ce chapitre contient les rubriques suivantes :

- Processus de session pour Horizon Help Desk Tool
- État de l'application pour Horizon Help Desk Tool
- Résoudre les problèmes de sessions de poste de travail et d’application dans Horizon Help Desk Tool

Démarrer Horizon Help Desk Tool dans la Horizon Console

Horizon Help Desk Tool est intégré à la Horizon Console. Vous pouvez rechercher un utilisateur pour lequel vous voulez résoudre des problèmes dans Horizon Help Desk Tool.

Procédure

1. Vous pouvez rechercher un nom d'utilisateur dans la zone de texte Recherche d'utilisateur ou accéder directement à l'outil Horizon Help Desk Tool.
   - Dans la Horizon Console, entrez un nom d'utilisateur dans la zone de texte Recherche d'utilisateur.
   - Sélectionnez **Surveiller > Service d'assistance** et entrez un nom d'utilisateur dans la zone de texte Recherche d'utilisateur.

   La Horizon Console affiche une liste d'utilisateurs dans les résultats de recherche. La recherche peut renvoyer jusqu'à 100 résultats correspondants.
2. Sélectionnez un nom d'utilisateur.

   Les informations d'utilisateur s'affichent dans une fiche utilisateur.

Étape suivante

Pour résoudre les problèmes, cliquez sur les onglets associés dans la fiche utilisateur.

Résolution des problèmes des utilisateurs dans Horizon Help Desk Tool

Dans Horizon Help Desk Tool, vous pouvez afficher des informations utilisateur de base dans une fiche utilisateur. Vous pouvez cliquer sur les onglets de la fiche utilisateur pour obtenir plus d’informations sur des composants spécifiques.

Les détails utilisateur peuvent parfois s'afficher dans des tableaux. Vous pouvez trier ces détails utilisateur dans des colonnes.

- Pour trier une colonne dans l'ordre croissant, cliquez une fois sur la colonne.
- Pour trier une colonne dans l'ordre décroissant, cliquez deux fois sur la colonne.
- Pour ne pas trier la colonne, cliquez trois fois sur la colonne.

Informations utilisateur de base

Affiche les informations utilisateur de base, telles que le nom, le numéro de téléphone et l'adresse e-mail de l'utilisateur, et indique si l'utilisateur est connecté ou déconnecté. Si l'utilisateur a ouvert une session de poste de travail ou d'application, l'état de l'utilisateur est Connecté. Dans le cas contraire, son état est Déconnecté.

Vous pouvez cliquer sur l'adresse e-mail pour envoyer un message à l'utilisateur.

Vous pouvez également cliquer sur le numéro de téléphone pour ouvrir une session Skype Entreprise pour appeler l'utilisateur afin de collaborer avec lui dans le cadre d'une tâche de dépannage.

Note Les informations de Skype Entreprise ne s'affichent pas pour les utilisateurs de postes de travail Linux.

Sessions

L'onglet **Sessions** affiche des informations sur les sessions de poste de travail ou d'applications auxquelles l'utilisateur est connecté.

Vous pouvez utiliser la zone de texte **Filtre** pour filtrer les sessions de poste de travail ou d'applications.

Note L'onglet **Sessions** n'affiche pas d'informations pour les sessions qui utilisent le protocole d'affichage Microsoft RDP ni pour les sessions qui accèdent aux machines virtuelles à partir de vSphere Client ou d'ESXi.

L'onglet **Sessions** contient les informations suivantes :

Tableau 14-1. Onglet Sessions

Option	Description
État	Affiche des informations sur l'état de la session de poste de travail ou d'application. ■ S'affiche en vert si la session est connectée. ■ L, si la session est une session locale ou une session en cours d'exécution dans l'espace local.
Nom de l'ordinateur	Nom de la session de poste de travail ou d'application. Cliquez sur le nom pour ouvrir les informations de session dans une fiche. Vous pouvez cliquer sur les onglets dans la carte de session pour afficher des informations supplémentaires : ■ L'onglet **Détails** affiche les informations utilisateur, telles que des informations sur la VM et l'utilisation du CPU ou de la mémoire. ■ L'onglet **Processus** affiche des informations sur les processus liés au CPU et à la mémoire. ■ L'onglet **Applications** affiche les détails sur les applications en cours d'exécution. **Note** Vous ne pouvez pas accéder à l'onglet **Applications** pour les sessions de poste de travail Linux.

Tableau 14-1. Onglet Sessions (suite)

Option	Description
Protocole	Protocole d'affichage de la session de poste de travail ou d'application.
Type	Indique si le poste de travail est un poste de travail publié, un poste de travail de machine virtuelle ou une application.
Heure d'ouverture de session	Heure à laquelle la session s'est connectée au Serveur de connexion.
Durée de la session	Durée de la connexion de la session au Serveur de connexion.

Postes de travail

L'onglet **Postes de travail** affiche des informations sur les postes de travail publiés ou les postes de travail virtuels que l'utilisateur est autorisé à utiliser.

Tableau 14-2. Postes de travail

Option	Description
État	Affiche des informations sur l'état de la session de poste de travail ■ S'affiche en vert si la session est connectée.
Nom du pool de postes de travail	Nom du pool de postes de travail de la session. Affiche Linux comme pool de postes de travail pour une session de poste de travail Linux.
Type de poste de travail	Indique si le poste de travail est un poste de travail publié ou un poste de travail de machine virtuelle. **Note** N'affiche pas d'informations si la session est en cours d'exécution dans un espace différent de la fédération d'espaces.
Type	Affiche des informations sur le type d'autorisation de poste de travail. ■ Locale, pour une autorisation locale.
vCenter	Affiche le nom de la machine virtuelle dans vCenter Server. **Note** N'affiche pas d'informations si la session est en cours d'exécution dans un espace différent de la fédération d'espaces.
Protocole par défaut	Protocole d'affichage par défaut de la session de poste de travail ou d'application.

Applications

L'onglet **Applications** affiche des informations sur les applications publiées que l'utilisateur est autorisé à utiliser.

Note Vous ne pouvez pas accéder à l'onglet **Applications** pour les sessions de poste de travail Linux.

Tableau 14-3. Applications

Option	Description
État	Affiche des informations sur l'état de la session d'application. ■ S'affiche en vert si la session est connectée.
Applications	Affiche les noms des applications publiées dans le pool d'applications.
Batterie de serveurs	Nom de la batterie de serveurs qui contient l'hôte RDS auquel la session se connecte. **Note** S'il existe un droit d'application global, cette colonne contient le nombre de batteries de serveurs dans ce droit.
Type	Affiche des informations sur le type d'autorisation d'application. ■ Locale, pour une autorisation locale.
Éditeur	Nom de l'éditeur du logiciel de l'application publiée.

Activités

L'onglet **Activités** affiche les informations de journal des événements sur les activités de l'utilisateur. Vous pouvez filtrer les activités selon un intervalle de temps, tel que les 12 dernières heures ou les 30 derniers jours, ou selon le nom de l'administrateur. Cliquez sur **Événement Service d'assistance uniquement** pour filtrer uniquement selon les activités d'Horizon Help Desk Tool. Cliquez sur l'icône d'actualisation pour actualiser le journal des événements. Cliquez sur l'icône d'exportation pour exporter le journal des événements en tant que fichier.

Note Le journal des événements n'est pas affiché pour les utilisateurs dans un environnement Architecture Cloud Pod.

Tableau 14-4. Activités

Option	Description
Heure	Sélectionnez un intervalle de temps. La valeur par défaut est les 12 dernières heures. ■ **12 dernières heures** ■ **24 dernières heures** ■ **7 derniers jours** ■ **30 derniers jours** ■ **Tout**
Administrateurs	Nom de l'utilisateur administrateur.
Message	Affiche les messages d'un utilisateur ou d'un administrateur qui sont spécifiques aux activités effectuées par l'utilisateur ou l'administrateur.
Nom de la ressource	Affiche les informations sur le nom du pool de postes de travail ou de la machine virtuelle sur lequel l'activité a été effectuée.

Détails de session d'Horizon Help Desk Tool

Les détails de session s'affichent dans l'onglet **Détails** lorsque vous cliquez sur un nom d'utilisateur dans l'option **Nom de l'ordinateur** dans l'onglet **Sessions**. Vous pouvez afficher les détails d'Horizon Client, le poste de travail virtuel ou publié et les détails du CPU et de la mémoire.

Horizon Client

Affiche des informations qui varient en fonction du type de client Horizon Client, ainsi que des détails tels que le nom d'utilisateur, la version d'Horizon Client, l'adresse IP et le système d'exploitation de la machine cliente.

Note Si vous avez mis Horizon Agent à niveau, vous devez également mettre à niveau Horizon Client vers la dernière version. Sinon, aucune version n'est affichée pour Horizon Client. Pour plus d'informations sur la mise à niveau d'Horizon Client, consultez le document *Mises à niveau d'Horizon 7*.

VM

Affiche des informations sur les postes de travail virtuels ou publiés.

Tableau 14-5. Détails de la machine virtuelle

Option	Description
Nom de l'ordinateur	Nom de la session de poste de travail ou d'application.
Version d'agent	Version de l'agent Horizon Agent.
Version du SE	Version du système d'exploitation.
Serveur de connexion	Serveur de connexion auquel la session se connecte.
Pool	Nom du pool de postes de travail ou d'applications. Affiche Linux pour un pool de postes de travail Linux.
vCenter	Adresse IP de vCenter Server.
État de session	État de la session de poste de travail ou d'application. Les états de session peuvent être inactif, actif ou déconnecté. Si l'utilisateur n'est pas actif pendant une minute, l'état de la session devient inactif. L'icône d'état apparaît avec un contour vert pour inactif, en vert uni pour actif et en gris pour déconnecté. **Note** Les sessions de poste de travail Linux n'affichent pas l'état inactif.
Durée de la session	Durée de connexion de la session au Serveur de connexion.
Durée de l'état	Durée de persistance de la session dans l'état.
Heure d'ouverture de session	Heure d'ouverture de session de l'utilisateur connecté à la session.
Durée d'ouverture de session	Durée de la connexion de l'utilisateur à la session.

Tableau 14-5. Détails de la machine virtuelle (suite)

Option	Description
Nom de la passerelle/du proxy	Nom du serveur de sécurité, du dispositif Unified Access Gateway ou de l'équilibrage de charge. L'affichage de ces informations peut prendre de 30 à 60 secondes après la connexion à la session.
Adresse IP de la passerelle/du proxy	Adresse IP du serveur de sécurité, du dispositif Unified Access Gateway ou de l'équilibrage de charge. L'affichage de ces informations peut prendre de 30 à 60 secondes après la connexion à la session.
Batterie de serveurs	Batterie d'hôtes RDS de la session d'application ou de poste de travail publié.

Mesures de l'expérience utilisateur

Affiche les détails de performances d'une session de poste de travail virtuel ou publié qui utilise le protocole d'affichage PCoIP ou VMware Blast. Pour afficher ces détails sur les performances, cliquez sur **Plus**. Pour actualiser ces détails, cliquez sur l'icône d'actualisation.

Tableau 14-6. Détails du protocole d'affichage PCoIP

Option	Description
Bande passante TX	Bande passante maximale, en kilobits par seconde, dans une session PCoIP.
Fréquence d'images	Fréquence d'images, en images par seconde, dans une session PCoIP.
Perte de paquets	Pourcentage de la perte de paquets dans une session PCoIP.
État de Skype	État de Skype Entreprise dans une session PCoIP. ■ Optimisé ■ Recours ■ Optimisé (incompatibilité de version) ■ Recours (incompatiblité de version) ■ Connexion ■ Déconnecté ■ Non défini Cette option indique S/O pour les sessions de poste de travail Linux.

Tableau 14-7. Détails du protocole d'affichage Blast

Option	Description
Fréquence d'images	Fréquence d'images, en images par seconde, dans une session Blast.
État de Skype	État de Skype Entreprise dans une session Blast. ■ Optimisé ■ Recours ■ Optimisé (incompatibilité de version) ■ Recours (incompatiblité de version) ■ Connexion ■ Déconnecté ■ Non défini Cette option indique S/O pour les sessions de poste de travail Linux.
Compteurs de session Blast	■ **Bande passante estimée (liaison montante)**. Bande passante estimée pour un signal de liaison montante. ■ **Perte de paquets (liaison montante)**. Pourcentage de perte de paquets pour un signal de liaison montante.
Compteurs d'imagerie Blast	■ **Octets transmis**. Nombre total d'octets pour les données d'imagerie qui ont été transmis pour une session Blast. ■ **Octets reçus**. Nombre total d'octets pour les données d'imagerie qui ont été reçus pour une session Blast.
Compteurs audio Blast	■ **Octets transmis**. Nombre total d'octets pour les données audio qui ont été transmis pour une session Blast. ■ **Octets reçus**. Nombre total d'octets pour les données audio qui ont été reçus pour une session Blast.
Compteurs CDR Blast	■ **Octets transmis**. Nombre total d'octets pour les données de redirection du lecteur client qui ont été transmis pour une session Blast. ■ **Octets reçus**. Nombre total d'octets pour les données de redirection du lecteur client qui ont été reçus pour une session Blast.

Utilisation du CPU et de la mémoire et performances du réseau et du disque

Affiche des graphiques de l'utilisation du CPU et de la mémoire de l'application ou du poste de travail virtuel ou publié et des performances du réseau ou du disque pour le protocole d'affichage PCoIP ou Blast.

Note Suite à un démarrage ou un redémarrage d'Horizon Agent sur le poste de travail, les graphiques de performances peuvent ne pas afficher immédiatement la chronologie. La chronologie s'affiche après quelques minutes.

Tableau 14-8. Utilisation du CPU

Option	Description
CPU de la session	Utilisation du CPU de la session actuelle.
CPU de l'hôte	Utilisation du CPU de la machine virtuelle à laquelle la session est attribuée.

Tableau 14-9. Utilisation de la mémoire

Option	Description
Mémoire de la session	Utilisation de la mémoire de la session actuelle.
Mémoire de l'hôte	Utilisation de la mémoire de la machine virtuelle à laquelle la session est attribuée.

Tableau 14-10. Performances du réseau

Option	Description
Latence	Affiche un graphique de la latence pour la session PCoIP ou Blast. Pour le protocole d'affichage Blast, le temps de latence est la durée de l'aller-retour en millisecondes. Le compteur de performances qui suit ce temps de latence est **Compteurs de session VMware Blast > RTT**. Pour le protocole d'affichage PCoIP, le temps de latence est la durée de latence aller-retour en millisecondes. Le compteur de performances qui suit ce temps de latence est **Statistiques de réseau de session PCoIP > Latence de parcours circulaire**.

Tableau 14-11. Performances du disque

Option	Description
Lecture	Nombre d'opérations d'entrée/sortie de lecture par seconde.
Écriture	Nombre d'opérations d'entrée/sortie d'écriture par seconde.
Latence de disque	Affiche un graphique de la latence de disque. La latence de disque est la durée en millisecondes des données IOPS (opérations d'entrée/sortie par seconde) récupérées depuis les compteurs de performances Windows.
Lecture moyenne	Nombre moyen d'opérations d'entrée/sortie de lecture aléatoire par seconde.
Écriture moyenne	Nombre moyen d'opérations d'entrée/sortie d'écriture aléatoire par seconde.
Latence moyenne	Temps de latence moyenne en millisecondes des données IOPS récupérées depuis les compteurs de performances Windows.

Segments d'ouverture de session

Affiche les segments de durée et d'utilisation de l'ouverture de session qui sont créés lors de l'ouverture de session.

Tableau 14-12. Segments d'ouverture de session

Option	Description
Durée d'ouverture de session	Durée calculée entre le moment où l'utilisateur clique sur le pool de postes de travail ou d'applications et le moment où l'Explorateur Windows démarre.
Heure d'ouverture de session	Durée de la connexion de l'utilisateur à la session.
Segments d'ouverture de session	Affiche les segments qui sont créés lors de l'ouverture de session. ■ **Intermédiation**. Délai total nécessaire au Serveur de connexion pour traiter une connexion ou une reconnexion à une session. Mesuré entre le moment où l'utilisateur clique sur le pool de postes de travail et le moment où la connexion par tunnel est configurée. Inclut les délais des tâches du Serveur de connexion, tels que l'authentification d'utilisateur, la sélection de machine et la préparation de la machine pour la configuration de la connexion par tunnel. ■ **Charge de GPO**. Délai total du traitement de la stratégie de groupe Windows. Affiche 0 si aucune stratégie globale n'est configurée. ■ **Charge de profil**. Délai total du traitement du profil d'utilisateur Windows. ■ **Interactif**. Délai total nécessaire à l'agent Horizon Agent pour traiter une connexion ou une reconnexion à une session. Mesuré entre le moment où PCoIP ou Blast Extreme utilise la connexion par tunnel et le moment où l'Explorateur Windows démarre. ■ **Connexion au protocole**. Durée totale nécessaire pour la connexion du protocole PCoIP ou Blast pendant le processus d'ouverture de session. ■ **Script d'ouverture de session**. Durée totale nécessaire pour l'exécution complète d'un script d'ouverture de session. ■ **Authentification**. Temps total dont dispose le Serveur de connexion pour authentifier la session. ■ **Démarrage de VM**. Temps total nécessaire pour démarrer une machine virtuelle. Cette durée inclut le temps de démarrage du système d'exploitation, la reprise d'une machine suspendue et le temps nécessaire à Horizon Agent pour signaler qu'il est prêt pour une connexion.

Suivez les instructions ci-dessous lorsque vous utilisez les informations des segments d'ouverture de session pour le dépannage :

- Si la session est une nouvelle session de poste de travail virtuel, tous les segments d'ouverture de session s'affichent. Si aucune stratégie globale n'est configurée, la durée du segment d'ouverture de session **Charge de GPO** est de 0.
- Si la session de poste de travail virtuel est une session reconnectée suite à sa déconnexion, les segments d'ouverture de session **Durée d'ouverture de session**, **Interactif** et **Intermédiation** s'affichent.

- Si la session est une session de poste de travail publié, les segments d'ouverture de session **Durée d'ouverture de session**, **Charge de GPO** ou **Charge de profil** s'affiche. Les segments d'ouverture de session **Charge de GPO** et **Charge de profil** s'affichent pour les nouvelles sessions. Si ces segments d'ouverture de session n'apparaissent pas pour les nouvelles sessions, vous devez redémarrer l'hôte RDS.
- Si la session est une session de poste de travail Linux, les segments **Charge de GPO** et **Charge de profil** ne s'affichent pas.
- Les données d'ouverture de session peuvent ne pas être immédiatement disponibles lorsque la session de poste de travail se connecte. Les données d'ouverture de session s'affichent après quelques minutes.

Processus de session pour Horizon Help Desk Tool

Les processus de session s'affichent dans l'onglet **Processus** lorsque vous cliquez sur un nom d'utilisateur dans l'option **Nom de l'ordinateur** dans l'onglet **Sessions**.

Processus

Pour chaque session, vous pouvez afficher des détails supplémentaires sur les processus liés au CPU et à la mémoire. Par exemple, si vous remarquez que l'utilisation du CPU et de la mémoire pour une session est anormalement élevée, vous pouvez afficher les détails pour le processus dans l'onglet **Processus**.

Pour les sessions hôtes RDS, l'onglet **Processus** affiche les processus de sessions hôtes RDS actuelles démarrés par l'utilisateur actuel ou le processus système actuel.

Tableau 14-13. Détails de processus de session

Option	Description
Nom du processus	Nom du processus de session. Par exemple, chrome.exe.
CPU	Utilisation du CPU du processus en pourcentage.
Mémoire	Utilisation de la mémoire du processus en Ko.
Disque	IOPS du disque de mémoire. Calculées avec la formule suivante : (Nombre total d'octets d'E/S de l'heure actuelle) - (Nombre total d'octets d'E/S une seconde avant l'heure actuelle). Ce calcul peut afficher une valeur de 0 Ko par seconde si le Gestionnaire des tâches affiche une valeur positive.
Nom d'utilisateur	Nom de l'utilisateur propriétaire du processus.
CPU de l'hôte	Utilisation du CPU de la machine virtuelle à laquelle la session est attribuée.
Mémoire de l'hôte	Utilisation de la mémoire de la machine virtuelle à laquelle la session est attribuée.
Processus	Nombre de processus dans la machine virtuelle

Tableau 14-13. Détails de processus de session (suite)

Option	Description
Actualiser	L'icône d'actualisation actualise la liste des processus.
Terminer le processus	Arrête un processus en cours d'exécution. **Note** Vous devez disposer du rôle Administrateur du service d'assistance pour terminer un processus. Pour mettre fin à un processus, sélectionnez un processus et cliquez sur le bouton **Terminer le processus**. Vous ne pouvez pas mettre fin aux processus critiques tels que les principaux processus Windows pouvant être répertoriés dans l'onglet **Processus**. Si vous arrêtez un processus critique, Horizon Help Desk Tool affiche un message indiquant qu'il ne peut pas terminer le processus système.

État de l'application pour Horizon Help Desk Tool

Vous pouvez afficher l'état et les détails d'une application dans l'onglet **Applications** lorsque vous cliquez sur un nom d'utilisateur dans l'option **Nom de l'ordinateur** dans l'onglet **Sessions**. Vous ne pouvez pas accéder à l'onglet **Applications** pour les sessions de poste de travail Linux.

Applications

Pour chaque application, vous pouvez afficher l'état actuel et d'autres détails.

Vous pouvez mettre fin à un processus d'application pour l'utilisateur final. Pour mettre fin à un processus d'application, cliquez sur **Mettre fin à l'application** et cliquez sur **OK** pour confirmer la modification.

Note Le processus de fin d'application peut échouer si l'application attend l'interaction d'un utilisateur, comme des données non enregistrées ou en raison d'autres exceptions. Toutefois, Horizon Help Desk Tool n'affiche aucun message de réussite ou d'échec lorsque vous mettez fin à une application.

Tableau 14-14. Détails de l'application

Option	Description
Application	Nom de l'application.
Description	Description de l'application.
État	État de l'application. Indique si l'application est en cours d'exécution ou pas.
CPU de l'hôte	Utilisation du CPU de la machine virtuelle à laquelle la session est attribuée.
Mémoire de l'hôte	Utilisation de la mémoire de la machine virtuelle à laquelle la session est attribuée.
Applications	Liste des applications en cours d'exécution.
Actualiser	L'icône d'actualisation actualise la liste des applications.

Résoudre les problèmes de sessions de poste de travail et d'application dans Horizon Help Desk Tool

Dans Horizon Help Desk Tool, vous pouvez résoudre les problèmes de sessions de poste de travail ou d'applications en fonction de l'état de la connexion de l'utilisateur.

Conditions préalables

- Démarrez Horizon Help Desk Tool.

Procédure

1. Dans la fiche utilisateur, cliquez sur l'onglet **Sessions**.

   Une fiche de performances indique l'utilisation du CPU et de la mémoire et contient des informations sur Horizon Client et le poste de travail virtuel ou publié.

2. Choisissez une option de dépannage.

Option	Action
Envoyer un message	Envoie un message à l'utilisateur sur le poste de travail publié ou le poste de travail virtuel. Vous pouvez choisir le niveau de gravité du message à inclure, à savoir Info, Avertissement ou Erreur. Cliquez sur **Envoyer un message**, entrez le type de gravité et les détails du message, puis cliquez sur **Envoyer**.
Assistance à distance	Vous pouvez générer des tickets d'assistance à distance pour les sessions connectées de poste de travail ou d'application. Les administrateurs peuvent utiliser le ticket d'assistance à distance pour prendre le contrôle du poste de travail d'un utilisateur et résoudre les problèmes. **Note** Cette fonctionnalité n'est pas disponible pour les utilisateurs de postes de travail Linux. Cliquez sur **Assistance à distance** et téléchargez le fichier de ticket Service d'assistance. Ouvrez le ticket et attendez que l'utilisateur l'accepte sur le poste de travail à distance. Vous pouvez ouvrir le ticket uniquement sur un poste de travail Windows. Une fois que l'utilisateur accepte le ticket, vous pouvez dialoguer avec lui et demander le contrôle de son poste de travail. **Note** La fonctionnalité d'assistance à distance Service d'assistance repose sur l'Assistance à distance Microsoft. Vous devez installer l'Assistance à distance Microsoft et activer la fonctionnalité d'assistance à distance sur le poste de travail publié. L'assistance à distance Service d'assistance ne démarre pas si l'Assistance à distance Microsoft rencontre des problèmes de connexion ou de mise à niveau. Pour plus d'informations, consultez la documentation de l'Assistance à distance Microsoft sur le site Web de Microsoft.

Option	Action
Redémarrer	Lance le processus de redémarrage de Windows sur le poste de travail virtuel. Cette fonctionnalité n’est pas disponible pour une session d'application ou de poste de travail publié. Cliquez sur **Redémarrer VDI**.
Se déconnecter	Déconnecte la session de poste de travail ou d’application. Cliquez sur **Plus > Se déconnecter**.
Fermer la session	Lance la déconnexion d’un poste de travail publié ou d’un poste de travail virtuel, ou d’une session d’application. Cliquez sur **Plus > Fermer la session**.
Réinitialiser	Initie une réinitialisation de la machine virtuelle. Cette fonctionnalité n’est pas disponible pour une session d'application ou de poste de travail publié. Cliquez sur **Plus > Réinitialiser la VM**. **Note** L’utilisateur peut perdre le travail non enregistré.

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.

Vous pouvez utiliser `vdmadmin` pour effectuer des tâches d'administration impossibles à réaliser dans l'interface utilisateur ou pour effectuer des tâches d'administration qui doivent s'exécuter automatiquement à partir de scripts.

- Utilisation de la commande vdmadmin

  La syntaxe de la commande `vdmadmin` contrôle son fonctionnement.

- 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.

- 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.

- 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.

- Liste et affichage de moniteurs de santé 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 Horizon 7 et pour afficher les détails d'un moniteur de santé ou d'une instance de moniteur spécifique.

- Liste et affichage de rapports sur le fonctionnement d'Horizon 7 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 Horizon 7 et pour afficher les résultats de l'exécution de ces rapports.

- Génération de messages du journal des événements d'Horizon 7 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 Horizon 7 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

  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

  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

  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

  Vous pouvez utiliser la commande `vdmadmin` avec l'option `-N` pour contrôler les domaines que Horizon 7 rend disponibles aux utilisateurs finaux.

- Configuration de filtres de domaine

  Vous pouvez configurer des filtres de domaine pour limiter les domaines qu'une instance du Serveur de connexion 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

  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

  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

  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 du Serveur de connexion 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 ou du serveur de sécurité de la configuration d'Horizon 7.

- 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.

- 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.

- 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 centre de données.

- Détection et résolution des collisions d'entrée et de schéma LDAP à l'aide de l'option -X

  Vous pouvez utiliser la commande `vdmadmin` avec l'option `-X` pour détecter et résoudre les collisions d'entrée LDAP et les collisions de schéma LDAP sur des instances du Serveur de connexion répliquées dans un groupe. Vous pouvez également utiliser cette option pour détecter et résoudre des collisions de schéma LDAP dans un environnement Architecture Cloud Pod.

Utilisation de la commande vdmadmin

La syntaxe de la commande `vdmadmin` contrôle son fonctionnement.

Utilisez la forme suivante de la commande `vdmadmin` à partir d'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 au 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

  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

  Certaines options de la commande `vdmadmin` vous permettent de spécifier le format des informations de sortie.

- 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.

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 Horizon Administrator pour attribuer le rôle **Administrateurs** à un utilisateur. Reportez-vous à la section #unique_9.

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.

Le tableau suivant 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.

Tableau 15-1. Options pour la sélection du format de sortie (suite)

Option	Description
–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.

Le tableau suivant montre les options de commande que vous pouvez utiliser avec la commande `vdmadmin` pour contrôler et vérifier le fonctionnement d'Horizon 7.

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. Remplace l'adresse IP signalée par Horizon Agent. Reportez-vous à la section Remplacement d'adresses IP à l'aide de l'option -A.
–C	Définit le nom d'un groupe Serveur de connexion. Reportez-vous à la section #unique_186.
–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.
–H	Affiche des informations sur la santé de services Horizon 7. Reportez-vous à la section Liste et affichage de moniteurs de santé à l'aide de l'option -H.
–I	Génère des rapports sur le fonctionnement de Horizon 7. Reportez-vous à la section Liste et affichage de rapports sur le fonctionnement d'Horizon 7 à l'aide de l'option -I.
–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.
–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.
–N	Configure les domaines qu'un groupe ou une instance du Serveur de connexion rend disponibles dans Horizon Client. Reportez-vous à la section Configuration de filtres de domaine à l'aide de l'option -N.
–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.
–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.
–Q	Configure le compte dans un compte Active Directory et la configuration de Horizon 7 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.
–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.
–S	Supprime de la configuration d'Horizon 7 une entrée de configuration correspondant à une instance du Serveur de connexion. Reportez-vous à la section Suppression de l'entrée pour une instance du Serveur de connexion ou un serveur de sécurité à l'aide de l'option -S.

Tableau 15-2. Options de la commande Vdmadmin (suite)

Option	Description
–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.
–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.
–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.
–X	Détecte et résout les entrées LDAP en double dans des instances du Serveur de connexion répliquées. Reportez-vous à la section Détection et résolution des collisions d'entrée et de schéma LDAP à l'aide de l'option -X.

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] -getlogfilelogfile-outfile local_file-d desktop-mmachine
```

```
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 [-mmachine]
```

```
vdmadmin
-A [-b authentication_arguments] -list [-xml] [-w | -n] -d desktop-m machine
```

```
vdmadmin
-A [-b authentication_arguments] -setloglevel level -ddesktop [-mmachine]
```

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

Le tableau suivant 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.

Tableau 15-3. Options pour configurer la journalisation dans Horizon Agent (suite)

Option	Description
`–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 bundle 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 [–bauthentication_arguments] –override–iip_or_dns–ddesktop–mmachine
```

```
vdmadmin
–A [–bauthentication_arguments] –override–list–ddesktop–mmachine
```

```
vdmadmin
–A [–bauthentication_arguments] –override–r–ddesktop [–mmachine]
```

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. Dans des configurations sécurisées où l'instance du Serveur de connexion 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

Le tableau suivant montre les options que vous pouvez spécifier pour remplacer les 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
```

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 [–bauthentication_arguments] [–udomain\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 de santé 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 Horizon 7 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] –monitoridmonitor_id –instanceid instance_id –xml [–w | –n]
```

Notes d'utilisation

Le tableau suivant indique les moniteurs de santé utilisés par Horizon 7 pour surveiller l'intégrité de ses composants.

Tableau 15-5. Moniteurs de santé

Moniteur	Description
CBMonitor	Contrôle l'intégrité des instances du Serveur de connexion.
DBMonitor	Contrôle l'intégrité de la base de données des événements.
DomainMonitor	Contrôle l'intégrité du domaine local et de tous les domaines approuvés de l'hôte du Serveur de connexion.
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, Horizon 7 crée une instance de moniteur distincte pour surveiller chaque instance du composant.

La commande émet toutes les informations sur les moniteurs de santé et les instances de contrôle au format XML.

Options

Le tableau suivant montre les options que vous pouvez spécifier pour répertorier et afficher des moniteurs de santé.

Tableau 15-6. Options pour répertorier et afficher des moniteurs de santé

Option	Description
`–instanceid` *instance_id*	Spécifie une instance de moniteur de santé.
`–list`	Affiche les moniteurs d'intégrité existants si aucun ID de moniteur de santé n'est spécifié.
`–list –monitorid` *monitor_id*	Affiche les instances de moniteur pour l'ID de moniteur de santé spécifié.
`–monitorid` *monitor_id*	Spécifie un ID de moniteur de santé.

Exemples

Répertoriez tous les moniteurs de santé 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 d'Horizon 7 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 Horizon 7 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 Horizon 7 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 Horizon 7 au format `syslog`. Reportez-vous à la section Génération de messages du journal des événements d'Horizon 7 au format Syslog à l'aide de l'option -I.

Options

Le tableau suivant 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 d'Horizon 7 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 Horizon 7 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 Horizon 7 au format `Syslog`. Dans un fichier `Syslog`, les messages du journal des événements de Horizon 7 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 d'Horizon 7 à l'aide de l'option -I.

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 Horizon 7 5.2 ou version ultérieure. Reportez-vous à la section « Configuration de la journalisation des événements pour des serveurs Syslog » dans le document *Installation d'Horizon 7*.

Tableau 15-8. Options de génération de messages de journal des événements d'Horizon 7 au format Syslog

Option	Description
`–disable`	Désactive la journalisation `Syslog`.
`–e|–enable`	Active la journalisation `Syslog`.
`–eventSyslog`	Spécifie que les événements de Horizon 7 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 Horizon 7 au format `Syslog`.

```
vdmadmin –I –eventSyslog –disable
```

Dirigez la sortie `Syslog` des événements de Horizon 7 vers le système local uniquement.

```
vdmadmin –I –eventSyslog –enable –localOnly
```

Dirigez la sortie `Syslog` des événements de Horizon 7 vers un chemin d'accès spécifié.

```
vdmadmin –I –eventSyslog –enable –path path
```

Dirigez la sortie `Syslog` des événements de Horizon 7 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 [–bauthentication_arguments] –ddesktop–m machine–udomain\user
```

```
vdmadmin
–L [–bauthentication_arguments] –ddesktop [–mmachine | –udomain\user] –r
```

Notes d'utilisation

Horizon 7 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 Horizon 7 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, ou pour modifier le propriétaire d'une machine virtuelle.

Dès qu'un utilisateur se connecte à un poste de travail distant attribué par Horizon 7 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.

Note La commande `vdmadmin -L` n'affecte pas la propriété à des disques persistants de View Composer. Pour attribuer des postes de travail de clone lié avec des disques persistants à des utilisateurs, utilisez l'option de menu **Attribuer un utilisateur** dans Horizon Administrator.

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

Le tableau suivant montre les options que vous pouvez spécifier pour attribuer un poste de travail à un utilisateur ou pour supprimer une attribution.

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 Horizon 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

Le tableau suivant 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 #unique_203.
- 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 Horizon 7 rend disponibles aux utilisateurs finaux.

Syntaxe

```
vdmadmin
```

```
        -N [-b authentication_arguments] -domains {-exclude | -include | -search} -domaindomain-add [-s
connsvr]
```

```
        vdmadmin
        -N [-b authentication_arguments] -domains-list [-w | -n] [-xml]
```

```
        vdmadmin
        -N [-bauthentication_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

Le tableau suivant 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.

Tableau 15-12. Options pour la configuration de filtres de domaine (suite)

Option	Description
`-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 ou pour le groupe Serveur de connexion.
`-list -active`	Affiche les domaines disponibles pour l'instance du Serveur de connexion 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. Vous pouvez spécifier l'instance du Serveur de connexion 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 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 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.

```
vdmadmin -N -domains -exclude -domain NEARDOM -add
```

Affichez la configuration de recherche de domaine sur les deux instances du Serveur de connexion 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 :
```

Horizon 7 limite la recherche de domaine sur chaque hôte du Serveur de connexion du groupe pour exclure les domaines FARDOM et DEPTX. Les caractères (*) en regard de la liste d'exclusion de CONSVR-1 indiquent que Horizon 7 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 Horizon 7 sur l'instance du Serveur de connexion.

```
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.

```
vdmadmin –N –domains –exclude –domain NEARDOM –remove
```

Supprimez tous les domaines de la liste d'inclusion pour l'instance du Serveur de connexion 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 ou un serveur de sécurité rend disponibles aux utilisateurs finaux.

Horizon 7 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 ou un serveur de sécurité. Pour un petit ensemble de domaines bien connectés, Horizon 7 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. Horizon 7 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 n'utilise que le domaine principal. Pour utiliser la fonctionnalité 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 sur laquelle vous avez défini cette clé.

Le tableau suivant 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 Horizon 7 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 Horizon 7 exclut des résultats d'une recherche de domaines. Vous ne pouvez pas exclure le domaine principal.
Liste d'inclusion	Spécifie les domaines que Horizon 7 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. Horizon 7 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.

2 Liste d'exclusion configurée pour le groupe Serveur de connexion.

3 Liste d'inclusion configurée pour l'instance du Serveur de connexion.

4 Liste d'inclusion configurée pour le groupe Serveur de connexion.

Horizon 7 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, Horizon 7 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 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 Horizon 7 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 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.

```
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 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
```

Horizon 7 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 qu'Horizon 7 exclut des résultats d'une recherche de domaine.

Un groupe de deux instances du Serveur de connexion, 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 dans le domaine MYDOM.

Affichez les domaines actuellement actifs d'un membre du groupe Serveur de connexion.

```
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.

```
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 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 :
```

Horizon 7 limite la recherche de domaine sur chaque hôte du Serveur de connexion du groupe pour exclure les domaines FARDOM et DEPTX. Les caractères (*) en regard de la liste d'exclusion de CONSVR-1 indiquent que Horizon 7 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 inactive. Vous voulez peut-être aussi examiner des règles qui sont affectées à des utilisateurs non autorisés.

Options

Le tableau suivant 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.
`-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. Feuilles de style XSL 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] [-groupgroup_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 dans le groupe qui contient l'instance du Serveur de connexion que les clients utilisent pour se connecter à leurs postes de travail distants.

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 dans un groupe.

Lorsque vous ajoutez un client en mode Kiosque, Horizon 7 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. Évitez d'utiliser ces préfixes avec des comptes d'utilisateur ordinaires.

Si vous ne spécifiez pas de nom pour un client, Horizon 7 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 du compte correspondant est cm-00_10_db_ee_76_80. Vous ne pouvez utiliser que ces comptes avec des instances du Serveur de connexion 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, Horizon 7 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 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, toutes les instances du Serveur de connexion 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 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 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 pour spécifier cette option, de tels clients ne peuvent pas s'authentifier eux-mêmes et ils échouent avec le message d'erreur `Nom d'utilisateur inconnu ou mot de passe incorrect`.

Options

Le tableau suivant 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 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 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. 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 sur lesquelles vous avez activé l'authentification de clients en mode kiosque.
`-noexpirepassword`	Spécifie que le mot de passe sur un compte n'expire pas.
`-nogroup`	Lors de l'ajout d'un compte pour un client, spécifie que le compte du client n'est pas ajouté au groupe par défaut. Lors de la définition des valeurs par défaut pour des clients, efface le paramètre du groupe par défaut.
`-ou` *DN*	Spécifie le nom unique de l'unité d'organisation à laquelle les comptes client sont ajoutés. Par exemple : OU=kiosk-ou,DC=myorg,DC=com **Note** Vous ne pouvez pas utiliser l'option `-setdefaults` pour modifier la configuration d'une unité d'organisation.
`-password` "*password*"	Spécifie un mot de passe explicite pour le compte du client.
`-remove`	Supprime le compte pour un client en mode kiosque.
`-removeall`	Supprime les comptes de tous les clients en mode kiosque.
`-requirepassword`	Spécifie que des clients en mode kiosque doivent fournir des mots de passe. Horizon 7 n'acceptera pas des mots de passe générés pour les nouvelles connexions.
`-s` *connection_server*	Spécifie le nom NetBIOS de l'instance du Serveur de connexion sur laquelle activer ou désactiver l'authentification de clients en mode kiosque.
`-setdefaults`	Définit les valeurs par défaut qui sont utilisées pour l'ajout de comptes client.
`-update`	Met à jour un compte pour un client en mode kiosque.

Exemples

Définissez les valeurs par défaut pour l'unité d'organisation, l'expiration du mot de passe et l'appartenance à un groupe de clients.

```
vdmadmin -Q -clientauth -setdefaults -ou "OU=kiosk-ou,DC=myorg,DC=com" -noexpirepassword -group kc-grp
```

Obtenez les valeurs par défaut actuelles de clients au format de texte brut.

```
vdmadmin -Q -clientauth -getdefaults
```

Obtenez les valeurs par défaut actuelles de clients au format XML.

```
vdmadmin –Q –clientauth –getdefaults –xml
```

Ajoutez un compte pour un client spécifié par son adresse MAC au domaine MYORG et utilisez les paramètres par défaut pour le groupe kc-grp.

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid 00:10:db:ee:76:80 –group kc–grp
```

Ajoutez un compte pour un client spécifié par son adresse MAC au domaine MYORG et utilisez un mot de passe généré automatiquement.

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid 00:10:db:ee:76:80 –genpassword –ou "OU=kiosk–
ou,DC=myorg,DC=com" –group kc–grp
```

Ajoutez un compte pour un client nommé et spécifiez un mot de passe à utiliser avec le client.

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid custom–Terminal21 –password "guest" –ou
"OU=kiosk–ou,DC=myorg,DC=com" –description "Terminal 21"
```

Mettez à jour un compte pour un client, en spécifiant un nouveau mot de passe et du texte descriptif.

```
vdmadmin –Q –clientauth –update –domain MYORG –clientid custom–Terminal21 –password "Secret1!" –
description "Foyer Entry Workstation"
```

Supprimez le compte pour un client kiosque spécifié par son adresse MAC du domaine MYORG.

```
vdmadmin –Q –clientauth –remove –domain MYORG –clientid 00:10:db:ee:54:12
```

Supprimez les comptes de tous les clients sans invite de confirmation de la suppression.

```
vdmadmin –Q –clientauth –removeall –force
```

Activez l'authentification de clients pour l'instance du Serveur de connexion csvr-2. Les clients avec des mots de passe générés automatiquement peuvent s'authentifier eux-mêmes sans fournir de mot de passe.

```
vdmadmin –Q –enable –s csvr–2
```

Activez l'authentification de clients pour l'instance du Serveur de connexion 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
```

Désactivez l'authentification de clients pour l'instance du Serveur de connexion csvr-1.

```
vdmadmin –Q –disable –s csvr–1
```

Affichez des informations sur des clients au format de texte. Le client cm-00_0c_29_0d_a3_e6 possède un mot de passe généré automatiquement et 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 CONSVR2 accepte les demandes d'authentification depuis des clients avec des mots de passe générés automatiquement. CONSVR1 n'accepte pas les demandes d'authentification depuis des clients en mode kiosque.

```
C:\ vdmadmin –Q –clientauth –list
Client Authentication User List
==============================
GUID              : 94be6344–0c9b–4a92–8d54–1brc1c2dc282
ClientID          : cm–00_0c_29_0d_a3_e6
Domain            : myorg.com
Password Generated: true

GUID              : 471d9d35–68b2–40ee–b693–56a7d92b2e25
ClientID          : cm–00_22_19_12_6d_cf
Domain            : myorg.com
Password Generated: false

Client Authentication Connection Servers
========================================
Common Name                   : CONSVR1
Client Authentication Enabled : false
Password Required             : false

Common Name                   : CONSVR2
Client Authentication Enabled : true
Password Required             : false
```

Affichage du premier utilisateur d'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.

Note 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 du Serveur de connexion 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 ou du serveur de sécurité de la configuration d'Horizon 7.

Syntaxe

```
        vdmadmin
        -S [-b authentication_arguments] -r-s server
```

Notes d'utilisation

Pour garantir une disponibilité élevée, Horizon 7 vous permet de configurer une ou plusieurs instances réplicas du Serveur de connexion dans un groupe Serveur de connexion. Si vous désactivez une instance du Serveur de connexion dans un groupe, l'entrée du serveur persiste dans la configuration d'Horizon 7.

Vous pouvez également utiliser la commande `vdmadmin` avec l'option `-S` pour supprimer un serveur de sécurité de votre environnement Horizon 7. 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 du Serveur de connexion ou le serveur de sécurité de l'ordinateur Windows Server en exécutant le programme d'installation du Serveur de connexion.

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 du Serveur de connexion, utilisez la commande `vdmadmin` pour supprimer de la configuration l'entrée pour l'instance du Serveur de connexion ou le serveur de sécurité désinstallé.

Si vous voulez réinstaller Horizon 7 sur les systèmes supprimés sans répliquer la configuration d'Horizon 7 du groupe d'origine, redémarrez tous les hôtes du Serveur de connexion dans le groupe d'origine avant d'effectuer la réinstallation. Cela évite aux instances réinstallées du Serveur de connexion de recevoir des mises à jour de configuration de leur groupe d'origine.

Options

L'option `-s` spécifie le nom NetBIOS de l'instance du Serveur de connexion ou du serveur de sécurité à supprimer.

Exemples

Supprimez l'entrée de l'instance du Serveur de connexion 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} -ownerdomain\user-userdomain\user [-passwordpassword]
```

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, vous devez fournir des informations d'identification secondaires aux utilisateurs administrateurs dans Horizon 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 Horizon 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 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)

Limites

- L'administration PowerShell et l'authentification par carte à puce des utilisateurs dans des domaines approuvés unidirectionnels ne sont pas prises en charge.
- L'authentification SAML des utilisateurs dans des domaines approuvés unidirectionnels n'est pas prise en charge.

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.

Tableau 15-17. Options pour fournir des informations d'identification secondaires (suite)

Option	Description
`–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 Horizon 7.

- 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 centre de données.

Syntaxe

```
vdmadmin
-V [-bauthentication_arguments] -e-ddesktop-mmachine [-m machine] ...
```

```
vdmadmin
-V [-bauthentication_arguments] -e-vcdnvCenter_dn-vmpath inventory_path
```

```
vdmadmin
-V [-b authentication_arguments] -p-d desktop -m machine [-mmachine] ...
```

```
vdmadmin
-V [-b authentication_arguments] -p-vcdnvCenter_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

Le tableau suivant 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 et de schéma LDAP à l'aide de l'option -X

Vous pouvez utiliser la commande `vdmadmin` avec l'option `–X` pour détecter et résoudre les collisions d'entrée LDAP et les collisions de schéma LDAP sur des instances du Serveur de connexion répliquées dans un groupe. Vous pouvez également utiliser cette option pour détecter et résoudre des collisions de schéma LDAP dans un environnement Architecture Cloud Pod.

Syntaxe

```
        vdmadmin
        –X [–bauthentication_arguments] –collisions [–resolve]
vdmadmin–X [–bauthentication_arguments] –schemacollisions [–resolve] [–global]
```

Notes d'utilisation

Des entrées LDAP en double dans au moins deux instances du Serveur de connexion peuvent entraîner des problèmes d'intégrité des données LDAP dans Horizon 7. Cela peut se produire au cours d'une mise à niveau alors que la réplication LDAP est inopérante. Bien qu'Horizon 7 recherche cette condition d'erreur à intervalles réguliers, vous pouvez exécuter la commande `vdmadmin` sur l'une des instances du Serveur de connexion du groupe pour détecter et résoudre manuellement les collisions d'entrées LDAP.

Les collisions de schéma LDAP peuvent également se produire au cours d'une mise à niveau alors que la réplication LDAP est inopérante. Comme Horizon 7 ne vérifie pas cette condition d'erreur, vous devez exécuter la commande `vdmadmin` pour détecter et résoudre des collisions de schéma LDAP manuellement.

Options

Le tableau suivant montre les options que vous pouvez spécifier pour détecter et résoudre des collisions d'entrée LDAP.

Tableau 15-19. Options pour la détection et la résolution des collisions d'entrée LDAP

Option	Description
`-collisions`	Spécifie une opération pour détecter des collisions d'entrée LDAP dans un groupe Serveur de connexion.
`-resolve`	Résout toutes les collisions LDAP dans l'instance LDAP. Si vous ne spécifiez pas cette option, la commande répertorie uniquement les problèmes qu'elle trouve.

Le tableau suivant montre les options que vous pouvez spécifier pour détecter et résoudre des collisions de schéma LDAP.

Tableau 15-20. Options pour la détection et la résolution des collisions de schéma LDAP

Option	Description
`-schemacollisions`	Spécifie une opération pour détecter des collisions de schéma LDAP dans un groupe Serveur de connexion ou un environnement Architecture Cloud Pod.
`-resolve`	Résout toutes les collisions de schéma LDAP dans l'instance LDAP. Si vous ne spécifiez pas cette option, la commande répertorie uniquement les problèmes qu'elle trouve.
`-global`	Applique les vérifications et les correctifs à l'instance LDAP globale dans un environnement Architecture Cloud Pod. Si vous ne spécifiez pas cette option, les vérifications sont exécutées par rapport à l'instance LDAP locale.

Exemples

Détecter des collisions d'entrée LDAP dans un groupe Serveur de connexion.

```
vdmadmin -X -collisions
```

Détecter et résoudre des collisions d'entrée LDAP dans l'instance LDAP locale.

```
vdmadmin -X -collisions -resolve
```

Détecter et résoudre des collisions de schéma LDAP dans l'instance LDAP globale.

```
vdmadmin -X -schemacollisions -resolve -global
```