Guide d'installation et de configuration de VMware Horizon Client pour Windows

VMware Horizon Client for Windows 2103

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

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

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

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

Table des matières

Guide d'installation et de configuration de VMware Horizon Client pour Windows 7

1 Configuration système requise et configuration pour clients basés sur Windows 8

Configuration système requise pour les systèmes clients Windows 8

Configuration système requise pour les fonctionnalités d'Horizon Client 11

Exigences de l'authentification par carte à puce 11

Exigences de l'authentification par certificat du périphérique client 13

Conditions requises pour l'intégration OPSWAT 14

Configuration système requise pour l'Audio/Vidéo en temps réel 14

Configuration système requise pour la redirection de scanner 15

Configuration système requise pour la redirection de port série 16

Configuration requise pour l'utilisation de la redirection de contenu URL 17

Configuration système requise pour la redirection multimédia HTML5 17

Configuration système requise pour la redirection de navigateur 19

Configuration système requise pour la redirection multimédia (MMR) 19

Configuration système requise pour la redirection de géolocalisation 20

Configuration requise pour la fonctionnalité de collaboration de session 21

Configuration requise pour l'utilisation de Skype Entreprise avec Horizon Client 22

Systèmes d'exploitation de poste de travail pris en charge 22

Préparation du Serveur de connexion pour Horizon Client 23

Effacement du dernier nom d'utilisateur utilisé pour se connecter à un serveur 25

Configurer des options VMware Blast 26

Utilisation des paramètres proxy d'Internet Explorer 28

Configurer le partage de données d'Horizon Client 29

Données Horizon Client collectées par VMware 29

2 Installation d'Horizon Client pour Windows 31

Activation du mode FIPS sur le système d'exploitation client Windows 31

Activation de la sélection automatique du protocole Internet 32

Installer Horizon Client pour Windows 33

Installation d'Horizon Client à partir de la ligne de commande 35

Commandes d'installation d'Horizon Client 36

Propriétés d'installation d'Horizon Client 36

Installation d'Horizon Client à partir de la ligne de commande 40

Vérifiez l'installation de Redirection de contenu URL 42

Mettre à jour Horizon Client en ligne 42

3 Configuration d'Horizon Client pour les utilisateurs finaux 45

Paramètres de configuration communs 45

Utilisation d'URI pour configurer Horizon Client 46

Syntaxe pour la création d'URI vmware-view 47

Exemples d'URI de vmware-view 51

Définition du mode de vérification des certificats dans Horizon Client 55

Configuration du mode de vérification des certificats pour les utilisateurs finaux 57

Configuration des options TLS avancées 58

Personnalisation des menus d'Horizon Client 58

Personnalisation des messages d'erreur d'Horizon Client 59

Configuration de la gestion des événements du curseur 59

Utilisation de paramètres de stratégie de groupe pour configurer Horizon Client 60

Paramètres de définition de scripts des objets de stratégie de groupe (GPO) des clients 61

Paramètres de sécurité des objets de stratégie de groupe (GPO) des clients 63

Paramètres RDP des objets de stratégie de groupe (GPO) des clients 71

Paramètres généraux des objets de stratégie de groupe (GPO) de clients 74

Paramètres USB des objets de stratégie de groupe (GPO) des clients 84

Paramètres de redirection de VMware Browser pour les objets de stratégie de groupe des clients 89

Paramètres de VMware Integrated Printing pour les GPO client 89

Paramètres de modèle d'administration ADMX pour les variables de session de client PCoIP 90

Exécution d'Horizon Client depuis la ligne de commande 95

Utilisation des commandes Horizon Client 96

Consulter le fichier de configuration Horizon Client 101

Utilisation du Registre Windows pour configurer Horizon Client 102

4 Gestion des connexions aux postes de travail distants et applications publiées 104

Se connecter à un poste de travail distant ou à une application publiée 104

Utiliser l'accès non authentifié pour se connecter à des applications publiées 108

Partager des informations d'emplacement 110

Masquer la fenêtre VMware Horizon Client 111

Reconnexion à un poste de travail distant ou une application publiée 112

Créer un raccourci sur le bureau du Client Windows ou dans le menu Démarrer 112

Utilisation des raccourcis créés par le serveur 113

Configurer les mises à jour des raccourcis du menu Démarrer 114

Configurer la fonction de connexion automatique pour un poste de travail distant 114

Fermer une session ou se déconnecter 115

Déconnexion d'un serveur 116

5 Travailler dans une application publiée ou un poste de travail distant 117

Prise en charge des fonctionnalités pour les clients Windows 118

Redimensionnement de la fenêtre du poste de travail distant 119

Écrans et résolution d'écran 119

Configurations à plusieurs moniteurs prises en charge 120

Sélectionner des moniteurs spécifiques pour afficher un poste de travail distant 121

Afficher un poste de travail distant sur un seul moniteur dans une configuration à plusieurs moniteurs 123

Sélectionner des moniteurs spécifiques pour afficher les applications publiées 123

Utiliser la mise à l'échelle de l'affichage 124

Utilisation de la synchronisation DPI 125

Modifier le mode d'affichage d'un poste de travail distant 127

Personnaliser la résolution et la mise à l'échelle de l'affichage pour un poste de travail distant 128

Utiliser des périphériques USB 130

Limitations de la redirection USB 132

Utilisation de webcams et de microphones 134

Lorsque vous pouvez utiliser une webcam avec la fonctionnalité Audio/Vidéo en temps réel 134

Sélectionner une webcam ou un microphone préféré sur un système client Windows 135

Utilisation de plusieurs périphériques avec la fonctionnalité audio/vidéo en temps réel 136

Sélectionner un haut-parleur préféré pour un poste de travail distant 137

Partage de sessions de poste de travail distant 138

Inviter un utilisateur à rejoindre une session de poste de travail distant 138

Gérer une session de poste de travail distant partagée 140

Rejoindre une session de poste de travail distant 141

Partager des lecteurs et des dossiers locaux 142

Ouvrir les fichiers locaux dans des applications publiées 146

Copier et coller 147

Copier et coller du texte et des images 147

Copier et coller des fichiers et des dossiers 148

Journalisation des activités copier et coller 149

Configuration de la taille de la mémoire du Presse-papiers du client 149

Glisser-déposer 150

Faire glisser du texte et des images 150

Glisser des fichiers et des dossiers 151

Conseils d'utilisation de la fonctionnalité de glisser-déposer 152

Conseils pour l'utilisation d'applications publiées 153

Se reconnecter aux applications publiées après une déconnexion 154

Utiliser plusieurs sessions d'une application publiée à partir de périphériques clients différents 155

Utiliser un IME (éditeur de méthode d'entrée) local avec des applications publiées 156

Impression à partir d'un poste de travail distant ou d'une application publiée 157
Définir les préférences d'impression de la fonctionnalité de VMware Integrated Printing 157
Impression à partir d'un poste de travail distant vers une imprimante USB locale 158
Améliorer les performances de la souris sur un poste de travail distant 159
Utilisation de scanners 160
Redirection des ports série 162
Raccourcis clavier 164
Synchronisation de la langue source d'entrée du clavier 167
Configurer la synchronisation des touches de verrouillage 168

6 Dépannage de Horizon Client 170
Redémarrer un poste de travail distant 170
Réinitialiser des postes de travail distants ou des applications publiées 171
Réparer Horizon Client pour Windows 172
Désinstaller Horizon Client pour Windows 173
Problèmes avec la saisie au clavier 174
Que faire si Horizon Client se ferme de façon inattendue 174
Connexion à un serveur en mode Workspace ONE 175

Guide d'installation et de configuration de VMware Horizon Client pour Windows

Ce guide décrit l'installation, la configuration et l'utilisation du logiciel VMware Horizon® Client™ sur un système client Microsoft Windows.

Ces informations sont conçues pour les administrateurs qui doivent configurer un déploiement d'Horizon comportant des systèmes clients Microsoft Windows, tels que des postes de travail et des ordinateurs portables. Les informations sont destinées aux administrateurs système expérimentés qui connaissent bien le fonctionnement des centres de données et de la technologie des machines virtuelles.

Si vous êtes utilisateur final, consultez le document *Guide de l'utilisateur de VMware Horizon Client pour Windows* ou affichez l'aide en ligne d'Horizon Client pour Chrome.

Configuration système requise et configuration pour clients basés sur Windows

1

Les systèmes exécutant des composants Horizon Client doivent respecter certaines exigences matérielles et logicielles.

Horizon Client sur des systèmes Windows utilise les paramètres Internet de Microsoft Internet Explorer, notamment des paramètres proxy, lors de la connexion à un serveur. Assurez-vous que vos paramètres Internet Explorer sont exacts et que vous pouvez accéder à l'URL du serveur via Internet Explorer.

Ce chapitre contient les rubriques suivantes :

- Configuration système requise pour les systèmes clients Windows
- Configuration système requise pour les fonctionnalités d'Horizon Client
- Configuration requise pour l'utilisation de Skype Entreprise avec Horizon Client
- Systèmes d'exploitation de poste de travail pris en charge
- Préparation du Serveur de connexion pour Horizon Client
- Effacement du dernier nom d'utilisateur utilisé pour se connecter à un serveur
- Configurer des options VMware Blast
- Utilisation des paramètres proxy d'Internet Explorer
- Configurer le partage de données d'Horizon Client

Configuration système requise pour les systèmes clients Windows

Vous pouvez installer Horizon Client pour Windows sur les ordinateurs de bureau et portables qui utilisent un système d'exploitation Microsoft Windows pris en charge.

L'ordinateur de bureau ou portable sur lequel vous installez Horizon Client, et les périphériques qu'il utilise, doit respecter une certaine configuration système.

Modèles

Tous les périphériques Windows x86-64 ou x86

Mémoire

Au moins 1 Go de RAM

Systèmes d'exploitation

Horizon Client prend en charge les systèmes d'exploitation suivants.

OS	Version	Service Pack ou option de service	Éditions prises en charge
Windows 10	32 bits ou 64 bits	Version 2009 SAC Version 2004 SAC Version 1909 SAC Entreprise 2019 LTSC Entreprise 2016 LTSC	Home, Pro, Pro for Workstations, Enterprise, Internet of Things (IoT) Enterprise et Éducation
Windows Server 2012 R2	64 bits	Dernière mise à jour	Standard et Datacenter
Windows Server 2016	64 bits	Dernière mise à jour	Standard et Datacenter
Windows Server 2019	64 bits	Dernière mise à jour	Standard et Datacenter

Windows Server 2012 R2, Windows Server 2016 et Windows Server 2019 sont pris en charge pour exécuter Horizon Client en mode imbriqué. Pour plus d'informations sur les fonctionnalités prises en charge en mode imbriqué, consultez l'article 67248 de la base de connaissances de VMware.

Important Parfois, les nouveaux systèmes d'exploitation Windows sont pris en charge après la publication de ce document. Pour obtenir les dernières informations concernant la prise en charge des systèmes d'exploitation, consultez l'article 58096 de la base de connaissances de VMware.

Serveur de connexion et Horizon Agent

Dernière version de maintenance d'Horizon 7 version 7.5.x et versions ultérieures.

Si des systèmes clients se connectent en dehors du pare-feu de l'entreprise, utilisez un dispositif Unified Access Gateway pour que les systèmes clients ne nécessitent pas de connexion VPN. Si votre société possède un réseau interne sans fil afin de permettre un accès routable aux postes de travail distants et si les périphériques peuvent utiliser ce réseau, il n'est pas nécessaire de configurer Unified Access Gateway ou une connexion VPN.

Protocoles d'affichage

- PCoIP
- VMware Blast
- RDP

Protocoles réseau

- IPv4
- IPv6

Lors d'une installation d'Horizon Client personnalisée, vous pouvez activer la sélection automatique du protocole Internet. Pour plus d'informations, reportez-vous à la section Activation de la sélection automatique du protocole Internet. Pour plus d'informations sur l'utilisation d'Horizon dans un environnement IPv6, consultez le document *Installation d'Horizon*.

Configuration matérielle requise pour PCoIP et VMware Blast

- Un processeur x86 avec extensions SSE2, avec une vitesse de processeur d'au moins 800 MHz.
- RAM disponible supérieure à la configuration requise pour prendre en charge plusieurs configurations d'écran. Utilisez la formule suivante comme indicateur général. L'unité de mesure est le pixel.

  ```
  20 MB + (24 * (# monitors) * (monitor width) * (monitor height))
  ```

  En général, vous pouvez utiliser les calculs suivants.

  ```
  1 monitor: 1600 x 1200: 64 MB
  2 monitors: 1600 x 1200: 128 MB
  3 monitors: 1600 x 1200: 256 MB
  ```

Exigences matérielles pour RDP

- Un processeur x86 avec extensions SSE2, avec une vitesse de processeur d'au moins 800 MHz.
- RAM de 128 Mo.

Exigences logicielles pour RDP

- Pour Windows 10, utilisez RDP 10.0.
- Le programme d'installation de l'agent configure la règle de pare-feu locale pour les connexions RDP entrantes afin qu'elle corresponde au port RDP actuel du système d'exploitation hôte, qui est en général le port 3389. Si vous modifiez le numéro du port RDP, vous devez modifier les règles de pare-feu associées.

Vous pouvez télécharger les versions de Remote Desktop Client sur le Centre de téléchargement de Microsoft.

Configuration requise pour les graphiques et la vidéo

- Carte graphique prenant en charge Direct3D 11 Video.
- Pilotes vidéo et de cartes graphiques les plus récents.

Configuration requise de .NET Framework

Le programme d'installation d'Horizon Client requiert .NET Framework version 4.5 ou ultérieure. Le programme d'installation vérifie si .NET Framework version 4.5 ou ultérieure est installé avant l'installation. Si la machine cliente ne répond pas à cette condition préalable, le programme d'installation télécharge automatiquement la dernière version de .NET Framework.

Configuration système requise pour les fonctionnalités d'Horizon Client

Les fonctionnalités d'Horizon Client présentent des exigences matérielles et logicielles spécifiques.

Exigences de l'authentification par carte à puce

Les périphériques clients qui utilisent une carte à puce pour l'authentification utilisateur doivent satisfaire certaines exigences.

Exigences logicielles et matérielles du client

Chaque périphérique client qui utilise une carte à puce pour l'authentification de l'utilisateur doit disposer des logiciels et matériels suivants.

- Horizon Client
- Un lecteur de carte à puce compatible

  Horizon Client prend en charge les cartes à puce et les lecteurs de carte à puce qui utilisent un fournisseur PKCS#11 ou Microsoft CryptoAPI. Facultativement, vous pouvez installer la suite logicielle ActivIdentity ActivClient qui fournit des outils pour interagir avec des cartes à puce.
- Des pilotes d'application spécifiques du produit

Les utilisateurs qui s'authentifient avec des cartes à puce doivent posséder une carte à puce ou un jeton de carte à puce USB, et chaque carte à puce doit contenir un certificat utilisateur.

Pour le fournisseur de services de chiffrement (CSP) spécifié dans le modèle d'émission de certificat, utilisez le fournisseur de services de chiffrement Microsoft pour carte à puce ou un CSP pour carte à puce tiers qui prend en charge RSA avec des algorithmes SHA-256.

Exigences de l'inscription par carte à puce

Pour installer des certificats sur une carte à puce, un administrateur doit configurer un ordinateur pour qu'il agisse comme une station d'inscription. Cet ordinateur doit avoir l'autorité d'émettre des certificats de carte à puce pour les utilisateurs, et il doit être membre du domaine pour lequel vous émettez des certificats.

Lorsque vous inscrivez une carte à puce, vous pouvez sélectionner la taille de clé du certificat résultant. Pour utiliser des cartes à puce avec des postes de travail locaux, vous devez sélectionner une clé de 1 024 bits ou de 2 048 bits lors de son inscription. Les certificats avec des clés de 512 bits ne sont pas pris en charge.

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.

Configuration logicielle requise pour les postes de travail distants et les applications publiées

Un administrateur Horizon doit installer les pilotes d'application spécifiques du produit sur les postes de travail virtuels ou sur l'hôte RDS.

Activation de la zone de texte Aide-mémoire du nom utilisateur dans Horizon Client

Dans certains environnements, les utilisateurs de carte à puce peuvent utiliser un seul certificat de carte à puce pour s'authentifier sur plusieurs comptes d'utilisateur. Les utilisateurs entrent leur nom d'utilisateur dans la zone de texte **Aide-mémoire du nom d'utilisateur** lorsqu'ils se connectent avec une carte à puce.

Pour que le champ **Aide-mémoire du nom d'utilisateur** apparaisse dans la boîte de dialogue de connexion d'Horizon Client, vous devez activer la fonctionnalité Aide-mémoire du nom d'utilisateur de carte à puce sur le Serveur de connexion. Pour plus d'informations sur l'activation de la fonctionnalité d'aide-mémoire du nom d'utilisateur de carte à puce, consultez le document *Administration d'Horizon*.

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 Unified Access Gateway, consultez le document *Déploiement et configuration de VMware Unified Access Gateway*.

Horizon Client prend toujours en charge les certificats de carte à puce de compte unique lorsque la fonctionnalité d'aide-mémoire du nom d'utilisateur de carte à puce est activée.

Exigences supplémentaires de l'authentification par carte à puce

Outre le respect des exigences de carte à puce pour les systèmes Horizon Client, les autres composants d'Horizon doivent également respecter certaines exigences de configuration pour prendre en charge les cartes à puce.

Hôtes du Serveur de connexion et du serveur de sécurité

Un administrateur doit ajouter toutes les chaînes de certificats d'autorité de certification (CA) applicables pour tous les certificats utilisateur de confiance à un fichier de magasin d'approbations de serveur sur l'hôte du Serveur de connexion ou, si un serveur de sécurité

est utilisé, sur l'hôte du serveur de sécurité. Ces chaînes de certificats incluent des certificats racines et, si une autorité de certification intermédiaire émet le certificat de carte à puce de l'utilisateur, elles doivent inclure également les certificats intermédiaires.

Pour plus d'informations sur la configuration du Serveur de connexion pour la prise en charge des cartes à puce, consultez le document*Administration d'Horizon*.

Dispositifs Unified Access Gateway

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

Active Directory

Pour plus d'informations sur les tâches qu'un administrateur peut effectuer dans Active Directory afin d'implémenter l'authentification par carte à puce, consultez le document *Administration d'Horizon*.

Exigences de l'authentification par certificat du périphérique client

Avec la fonctionnalité d'authentification par certificat du périphérique client, vous pouvez configurer l'authentification par certificat pour les périphériques clients. Unified Access Gateway authentifie les périphériques clients. Microsoft Certificate Services, avec Active Directory, gère la création et la distribution des certificats sur les périphériques clients. Une fois l'authentification du périphérique effectuée, l'utilisateur doit toujours exécuter l'authentification de l'utilisateur.

Cette fonction a les exigences suivantes :

- Unified Access Gateway 2.6 ou version ultérieure
- Horizon 7 version 7.5 ou version ultérieure
- Un certificat installé sur le périphérique client qui est accepté par Unified Access Gateway

Pour plus d'informations sur la configuration d'Unified Access Gateway, consultez la documentation d'Unified Access Gateway.

Pour le fournisseur de services cryptographiques (CSP) spécifié dans le modèle d'émission de certificat, utilisez Microsoft Enhanced RSA and AES Cryptographic Provider. Ce CSP prend en charge les certificats SHA-256 et TLS v1.2. Utilisez SHA-256. SHA-1 est trop faible pour l'authentification.

Pour que Windows utilise un certificat pour l'authentification du périphérique client, l'utilisateur sur le périphérique client doit disposer d'un accès en lecture à la clé privée du certificat. La clé privée n'a pas besoin d'être exportable. L'utilisation de la clé du certificat doit inclure la signature numérique et le chiffrement de clé (a0).

Vous pouvez installer le certificat dans le magasin de certificats Utilisateur actuel ou Ordinateur local sur le périphérique client. Sous Windows 10, si vous installez le certificat dans le magasin de certificats Ordinateur local et que l'utilisateur n'appartient pas au groupe d'utilisateurs SYSTÈME ou Administrateurs locaux, vous devez effectuer les étapes suivantes pour donner à l'utilisateur l'accès en lecture à la clé privée du certificat. Si vous installez le certificat dans le magasin de certificats Utilisateur actuel, vous n'avez pas besoin d'effectuer ces étapes.

1 Ouvrez le magasin de certificats Ordinateur local sur le périphérique client.

2 Cliquez avec le bouton droit sur le certificat du périphérique et sélectionnez **Toutes les tâches > Gérer les clés privées**.

3 Ajoutez l'utilisateur, attribuez une autorisation de lecture à l'utilisateur, puis cliquez sur **OK**.

Conditions requises pour l'intégration OPSWAT

Dans certaines entreprises, un administrateur peut intégrer Unified Access Gateway à l'application MetaAccess OPSWAT tierce. Cette intégration, qui est généralement utilisée sur des périphériques non gérés dans des environnements BYOD d'entreprise, permet aux organisations de définir des stratégies d'acceptation de périphérique pour les périphériques Horizon Client.

Par exemple, un administrateur peut définir une stratégie d'acceptation de périphérique qui exige que les périphériques clients soient protégés par mot de passe ou disposent d'une version de système d'exploitation minimale. Les périphériques client conformes à la stratégie d'acceptation de périphérique peuvent accéder aux postes de travail distants et aux applications publiées via Unified Access Gateway. Unified Access Gateway refuse l'accès aux ressources distantes des périphériques clients qui ne sont pas conformes à la stratégie d'acceptation de périphérique.

Pour plus d'informations, consultez le document *Déploiement et configuration de VMware Unified Access Gateway*.

Configuration système requise pour l'Audio/Vidéo en temps réel

La fonctionnalité Audio/Vidéo en temps réel fonctionne avec des webcams standard, audio USB et des périphériques audio analogiques. La fonctionnalité fonctionne également avec les applications de conférence standard. Pour prendre en charge l'Audio/Vidéo en temps réel, votre déploiement d'Horizon doit satisfaire certaines exigences matérielles et logicielles.

Postes de travail virtuels

Pour utiliser plus d'une webcam ou d'un microphone dans un poste de travail virtuel, Horizon Agent 7.10 ou version ultérieure doit être installé.

Lorsque vous utilisez Microsoft Teams avec la fonctionnalité d'Audio/Vidéo en temps réel, les postes de travail virtuels doivent disposer d'au moins 4 vCPU et 4 Go de RAM.

Ordinateur Horizon Client ou périphérique d'accès client

- L'Audio/Vidéo en temps réel est pris en charge par tous les systèmes d'exploitation client Windows qui utilisent Horizon Client pour Windows. Pour plus d'informations, reportez-vous à la section Configuration système requise pour les systèmes clients Windows.

- Les pilotes des webcams et des périphériques audio doivent être installés, et la webcam ainsi que le périphérique audio doivent être opérationnels sur l'ordinateur client. Vous n'avez pas besoin d'installer les pilotes de périphérique sur la machine sur laquelle l'agent est installé.

Protocoles d'affichage

- PCoIP
- VMware Blast

Configuration système requise pour la redirection de scanner

Les utilisateurs finaux peuvent scanner des informations vers leurs applications et postes de travail distants avec des scanners connectés à leurs systèmes clients locaux. Pour utiliser cette fonctionnalité, les postes de travail distants et les ordinateurs clients doivent répondre à certaines configurations système requises.

Postes de travail distants

Les postes de travail distants nécessitent l'installation d'Horizon Agent, avec l'option de configuration de redirection de scanner sélectionnée, sur les machines virtuelles parentes ou modèles, ou sur les hôtes RDS. Sur les systèmes d'exploitation de poste de travail Windows et invités Windows Server, l'option de configuration de redirection de scanner d'Horizon Agent est désélectionnée par défaut.

Pour plus d'informations sur les systèmes d'exploitation invités pris en charge sur les postes de travail virtuels et les hôtes RDS, ainsi que sur la configuration de la redirection de scanner dans les applications publiées et les postes de travail distants, consultez la section « Configuration de redirection de scanner » dans le document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Ordinateur Horizon Client ou périphérique d'accès client

La redirection de scanner est prise en charge sur Windows 10. Les pilotes du scanner doivent être installés, et ce dernier doit être opérationnel sur l'ordinateur client. Vous n'avez pas besoin d'installer les pilotes du scanner sur le système d'exploitation du poste de travail à distance sur lequel l'agent est installé.

Norme de scanner

TWAIN ou WIA

Protocoles d'affichage

- PCoIP
- VMware Blast

La redirection de scanner n'est pas prise en charge dans les sessions de poste de travail RDP.

Configuration système requise pour la redirection de port série

Avec la fonctionnalité de redirection de port série, les utilisateurs finaux peuvent rediriger des ports série (COM) connectés en local, tels que les ports RS232 intégrés ou des adaptateurs USB-série, vers leurs postes de travail distants et leurs applications publiées. Pour prendre en charge la redirection de port série, votre déploiement de VMware Horizon doit répondre à certaines exigences matérielles et logicielles.

Postes de travail virtuels

Vous devez installer Horizon Agent avec l'option de configuration de redirection de port série sélectionnée. Cette option d'installation n'est pas sélectionnée par défaut.

Les systèmes d'exploitation suivants sont pris en charge sur les postes de travail virtuels.

- Windows 7 64 bits
- Windows 8.x 64 bits
- Windows 10 64 bits
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

Note Horizon Agent 2006 et version ultérieure ne prend pas en charge Windows 7, Windows 8.x, Windows Server 2008 R2 et Windows Server 2012 R2.

Il n'est pas nécessaire d'installer les pilotes de périphériques de port série sur le poste de travail virtuel.

Postes de travail publiés et applications publiées

Horizon Agent 7.6 ou version ultérieure doit être installé sur les hôtes RDS avec l'option de configuration de la redirection de port série sélectionnée. Cette option d'installation n'est pas sélectionnée par défaut.

Les systèmes d'exploitation suivants sont pris en charge pour les postes de travail publiés et les applications publiées.

- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

Note Horizon Agent 2006 et version ultérieure ne prend pas en charge Windows Server 2008 R2 et Windows Server 2012 R2.

Il n'est pas nécessaire d'installer les pilotes de périphériques de port série sur l'hôte RDS.

La redirection de port série est disponible avec des postes de travail complets et n'est pas prise en charge sur les applications publiées sur les hôtes RDS.

Ordinateur Horizon Client ou périphérique d'accès client

La redirection de port série est prise en charge sur les systèmes clients Windows 10. Tous les pilotes de périphérique de port série nécessaires doivent être installés et le port série doit être opérationnel.

Protocoles d'affichage

- PCoIP
- VMware Blast

La redirection de port série n'est pas prise en charge dans les sessions de poste de travail RDP.

Pour plus d'informations sur la configuration de la redirection de port série, reportez-vous à la section « Configuration de la redirection de port série » dans le document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Configuration requise pour l'utilisation de la redirection de contenu URL

Avec la fonctionnalité de redirection de contenu URL, le contenu URL peut être redirigé à partir de la machine cliente vers une application publiée ou un poste de travail distant (redirection client vers agent), ou à partir d'une application publiée ou d'un poste de travail distant vers la machine cliente (redirection agent vers client).

Par exemple, un utilisateur final peut cliquer sur un lien de l'application Microsoft Word native sur le client pour que le lien s'ouvre dans l'application Internet Explorer distante. L'utilisateur final peut également cliquer sur un lien dans l'application Internet Explorer distante. Le lien s'ouvre alors dans un navigateur natif sur la machine cliente. Vous pouvez configurer un nombre quelconque de protocoles pour la redirection, notamment HTTP, mailto et callto.

Un administrateur Horizon doit également configurer des paramètres qui spécifient comment Horizon Client redirige le contenu URL à partir du client vers une application publiée ou un poste de travail distant, ou comment Horizon Agent redirige le contenu URL à partir d'une application publiée ou d'un poste de travail distant vers le client.

Pour plus d'informations, consultez la rubrique « Configuration de la redirection de contenu URL » dans le document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Configuration système requise pour la redirection multimédia HTML5

Horizon Agent et Horizon Client, ainsi que les postes de travail distants et les systèmes clients sur lesquels vous installez les logiciels agent et client doivent respecter la configuration système requise pour la prise en charge de la fonctionnalité de redirection multimedia HTML5.

Avec la redirection multimédia HTML5, si un utilisateur final utilise le navigateur Google Chrome ou Microsoft Edge sur un poste de travail distant, le contenu multimédia HTML5 est transmis au système client. Le système client lit le contenu multimédia, ce qui réduit la charge sur l'hôte ESXi, et l'utilisateur final peut profiter d'une meilleure expérience audio et vidéo.

Poste de travail distant

- Vous devez installer Horizon Agent sur le poste de travail virtuel ou sur l'hôte RDS pour les postes de travail publiés avec l'option de configuration personnalisée de redirection multimédia HTML5 sélectionnée. À partir d'Horizon Agent 7.10, l'option d'installation personnalisée de la redirection multimédia HTML5 est supprimée et la redirection multimédia HTML5 est installée par défaut. Pour plus d'informations, consultez les rubriques sur l'installation d'Horizon Agent dans les documents *Configuration des postes de travail virtuels dans Horizon* et *Configuration d'applications et de postes de travail publiés dans Horizon*.
- Les paramètres de stratégie de groupe de redirection multimédia HTML5 doivent être configurés sur le serveur Active Directory. Consultez les rubriques sur la configuration de la redirection multimédia HTML5 dans le document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.
- Le navigateur Chrome ou Edge doit être installé.
- L'extension de redirection multimédia HTML5 de VMware Horizon doit être installée dans le navigateur Chrome ou Edge. Consultez les rubriques sur la configuration de la redirection multimédia HTML5 dans le document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Système client

- La prise en charge de la redirection multimédia HTML5 et de l'option d'installation personnalisée de redirection de navigateur doit être sélectionnée lorsque vous installez Horizon Client. Cette option est sélectionnée par défaut.

Protocole d'affichage de la session distante

- PCoIP
- VMware Blast

Port TCP

La redirection multimédia HTML5 utilise le port 9427.

Limites

La fonctionnalité de redirection multimédia HTML5 présente les limitations suivantes.

- La fonctionnalité de souris relative Horizon Client n'est pas prise en charge.
- Vous ne pouvez pas utiliser **Couper le son du site** (navigateur Chrome) ou **Couper le son de l'onglet** (navigateur Edge) pour désactiver le contenu vidéo redirigé.

Configuration système requise pour la redirection de navigateur

Les postes de travail distants et les systèmes clients sur lesquels vous installez les logiciels agent et client doivent respecter la configuration requise pour la prise en charge de la fonctionnalité Redirection de navigateur.

Grâce à la redirection de navigateur, lorsqu'un utilisateur final ouvre un site Web dans le navigateur Chrome sur un poste de travail distant, la page Web est restituée sur le système client plutôt que sur le système agent, et elle est affichée sur la fenêtre d'affichage du navigateur distant. La fenêtre d'affichage est la partie de la fenêtre du navigateur qui contient le contenu de la page Web.

Postes de travail distants

- Vous devez installer Horizon Agent 7.10 ou version ultérieure sur le poste de travail virtuel ou l'hôte RDS pour les postes de travail publiés. Consultez les rubriques sur l'installation Horizon Agent dans les documents *Configuration des postes de travail virtuels dans Horizon* et *Configuration d'applications et de postes de travail publiés dans Horizon*.
- Les paramètres de stratégie de groupe de Redirection de VMware Browser doivent être configurés sur le serveur Active Directory. Consultez les rubriques sur la configuration de la redirection de navigateur dans le document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.
- Le navigateur Chrome doit être installé.
- L'extension de redirection de navigateur VMware Horizon doit être installée dans le navigateur Chrome. Consultez les rubriques sur la configuration de la redirection de navigateur dans le document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Protocole d'affichage de la session distante

- PCoIP
- VMware Blast

Configuration système requise pour la redirection multimédia (MMR)

La redirection multimédia (MMR) permet de décoder le flux multimédia sur le système client. Le système client effectue la lecture du contenu multimédia, ce qui réduit la charge sur l'hôte ESXi.

Postes de travail distants

Pour plus d'informations sur la configuration système requise pour le système d'exploitation et les autres exigences logicielles et paramètres de configuration, consultez les rubriques sur la redirection multimédia Windows Media dans le document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Ordinateur Horizon Client ou périphérique d'accès client

Windows 10

Formats multimédias pris en charge

Les formats multimédias pris en charge par le lecteur Windows Media, par exemple : M4V ; MOV ; MP4 ; WMP ; MPEG-4 Part 2 ; WMV 7, 8 et 9 ; WMA ; AVI ; ACE ; MP3 ; WAV.

MP3 n'est pas pris en charge lors de l'utilisation de MMS et de RTSP.

Note Le contenu protégé par DRM n'est pas redirigé via la Redirection multimédia du Lecteur Windows Media.

Configuration système requise pour la redirection de géolocalisation

Horizon Agent et Horizon Client, ainsi que le poste de travail virtuel ou l'hôte RDS et la machine cliente sur lesquels vous installez les logiciels agent et client doivent respecter la configuration requise pour la prise en charge de la fonctionnalité de redirection de géolocalisation.

Avec la redirection de géolocalisation, les informations de géolocalisation sont envoyées depuis le système client vers le poste de travail distant ou l'application publiée.

Poste de travail virtuel ou hôte RDS

- Le paramètre **Service d'emplacement** de Windows doit être **activé** dans **Paramètres > Confidentialité > Emplacement**.
- La fonctionnalité de redirection de géolocalisation prend en charge les applications de poste de travail distant suivantes.

Application	Plate-forme
Google Chrome (dernière version)	Tous les postes de travail virtuels ou hôtes RDS
Internet Explorer 11	Tous les postes de travail virtuels ou hôtes RDS
Edge, Maps, Météo et autres applications Win32 et UWP	Windows 10

  Le paramètre d'autorisation **Emplacement**, le cas échéant, doit être activé individuellement dans chaque navigateur pris en charge.
- Horizon Agent 7.6 ou version ultérieure doit être installé avec l'option de configuration personnalisée de redirection de géolocalisation sélectionnée. Cette option n'est pas sélectionnée par défaut. Consultez les rubriques sur l'installation Horizon Agent dans les documents *Configuration des postes de travail virtuels dans Horizon* et *Configuration d'applications et de postes de travail publiés dans Horizon*.
- Les paramètres de stratégie de groupe de redirection de géolocalisation VMware doivent être configurés sur le serveur Active Directory. Consultez les rubriques sur la configuration de la redirection de géolocalisation dans le document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.
- Pour Internet Explorer 11, vous devez activer le plug-in IE de géolocalisation VMware Horizon pour les hôtes RDS. Il n'est pas nécessaire d'activer le plug-in IE de redirection de

géolocalisation VMware Horizon pour les postes de travail virtuels Windows 10. Internet Explorer est pris en charge sur les postes de travail virtuels Windows 10 avec le pilote de redirection de géolocalisation de VMware. Consultez les rubriques sur la configuration de la redirection de géolocalisation dans le document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

- Pour Chrome, le plug-in Chrome de redirection de géolocalisation VMware Horizon doit être activé. Consultez les rubriques sur la configuration de la redirection de géolocalisation dans le document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Système client

- Pour partager des informations sur l'emplacement du système client, vous devez configurer les paramètres **Géolocalisation** dans Horizon Client. Pour plus d'informations, consultez Partager des informations d'emplacement.
- Pour les systèmes clients Windows 10, le paramètre de service **Emplacement** Windows doit être **activé** dans **Paramètres > Confidentialité > Emplacement** pour qu'Horizon accède à votre emplacement.

Protocole d'affichage de la session distante

- PCoIP
- VMware Blast

Configuration requise pour la fonctionnalité de collaboration de session

Avec la fonctionnalité de collaboration de session, les utilisateurs peuvent inviter d'autres utilisateurs à rejoindre une session de poste de travail distante existante. Pour prendre en charge la fonctionnalité de collaboration de session, votre déploiement d'Horizon doit satisfaire certaines exigences.

Collaborateurs de session

Pour rejoindre une session de collaboration, l'utilisateur doit disposer d'Horizon Clientpour Windows, Mac ou Linux installé sur le système client ou utiliser HTML Access.

Postes de travail distants Windows

La fonctionnalité de collaboration de session doit être activée au niveau du pool de postes de travail ou de la batterie de serveurs. Pour plus d'informations sur l'activation de la fonctionnalité de collaboration de session pour des pools de postes de travail, consultez le document *Configuration des postes de travail virtuels dans Horizon*. Pour plus d'informations sur l'activation de la fonctionnalité de collaboration de session pour une batterie de serveurs, consultez le document *Configuration d'applications et de postes de travail publiés dans Horizon*.

Vous pouvez utiliser les paramètres de stratégie de groupe Horizon Agent pour configurer la fonctionnalité de collaboration de session. Pour plus d'informations, consultez le document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Postes de travail à distance Linux

Pour connaître les exigences des postes de travail distants Linux, consultez le document *Configuration des postes de travail Linux dans Horizon*.

Serveur de connexion

La fonctionnalité de collaboration de session requiert que l'instance du Serveur de connexion utilise une licence d'entreprise.

Protocoles d'affichage

VMware Blast

La fonctionnalité de collaboration de session ne prend pas en charge les sessions d'application publiée.

Configuration requise pour l'utilisation de Skype Entreprise avec Horizon Client

Un utilisateur final peut exécuter Skype Entreprise sur un poste de travail virtuel sans affecter l'infrastructure virtuelle et sans entraîner de surcharge du réseau. Au cours des appels audio et vidéo Skype, tous les processus multimédias ont lieu sur la machine cliente plutôt que sur le poste de travail virtuel.

Pour utiliser cette fonctionnalité, vous devez installer le pack de virtualisation pour la fonctionnalité Skype Entreprise sur la machine cliente lors de l'installation d'Horizon Client pour Windows. Pour plus d'informations, reportez-vous à la section Chapitre 2 Installation d'Horizon Client pour Windows.

Un administrateur Horizon doit également installer le pack de virtualisation VMware pour Skype Entreprise sur le poste de travail virtuel lors de l'installation d'Horizon Agent. Pour plus d'informations sur l'installation de Horizon Agent, reportez-vous au document *Configuration des postes de travail virtuels dans Horizon*.

Pour plus d'informations sur les exigences, reportez-vous à la section « Configurer Skype Entreprise » dans le document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Systèmes d'exploitation de poste de travail pris en charge

Un administrateur Horizon crée des machines virtuelles qui disposent d'un système d'exploitation invité et installe le logiciel agent dans le système d'exploitation invité. Les utilisateurs finaux peuvent ouvrir une session sur ces machines virtuelles à partir d'un périphérique client.

Pour obtenir une liste des systèmes d'exploitation invités Windows pris en charge, consultez le document *Installation d'Horizon*.

Certains systèmes d'exploitation invités Linux sont également pris en charge. Pour plus d'informations sur la configuration système requise, la configuration des machines virtuelles Linux et la liste des fonctionnalités prises en charge, consultez le document *Configuration des postes de travail Linux dans Horizon*.

Préparation du Serveur de connexion pour Horizon Client

Pour que les utilisateurs finaux puissent se connecter à un serveur et accéder à un poste de travail distant ou une application publiée, un administrateur Horizon doit configurer certains paramètres du Serveur de connexion.

Unified Access Gateway et serveurs de sécurité

Si votre déploiement de VMware Horizon inclut un dispositif Unified Access Gateway, configurez le Serveur de connexion pour qu'il fonctionne avec Unified Access Gateway. Reportez-vous au document *Déploiement et configuration de VMware Unified Access Gateway*. Les dispositifs Unified Access Gateway jouent le même rôle en tant que les serveurs de sécurité.

Si votre déploiement de VMware Horizon inclut un serveur de sécurité, vérifiez que vous utilisez les dernières versions de maintenance du Serveur de connexion 7.5.x et du Serveur de sécurité 7.5.x ou versions ultérieures. Pour plus d'informations, reportez-vous au document d'installation de votre version d'Horizon.

Note Les serveurs de sécurité ne sont pas pris en charge dans VMware Horizon 2006 et version ultérieure.

Connexion par tunnel sécurisé

Si vous prévoyez d'utiliser une connexion par tunnel sécurisé pour les périphériques clients et si la connexion sécurisée est configurée avec un nom d'hôte DNS pour une instance du Serveur de connexion ou un serveur de sécurité, vérifiez que le périphérique client peut résoudre ce nom DNS.

Pools de postes de travail et d'applications

Utilisez la liste de vérification suivante lors de la configuration de pools de postes de travail et d'applications.

- Vérifiez qu'un pool de postes de travail ou d'applications a été créé et que le compte d'utilisateur que vous souhaitez utiliser est autorisé à accéder au pool. Pour plus d'informations, consultez les documents *Configuration des postes de travail virtuels dans Horizon* et *Configuration d'applications et de postes de travail publiés dans Horizon*.

- Si les utilisateurs finaux disposent d'un écran haute résolution et s'ils utilisent le paramètre client **Mode haute résolution** lors de l'affichage de leurs poste de travail distants en mode plein écran, vérifiez que suffisamment de mémoire vRAM est allouée pour chaque poste de travail distant Windows. La quantité de vRAM dépend de la résolution d'affichage et du nombre de moniteurs configurés pour les utilisateurs finaux.

Authentification des utilisateurs

Utilisez la liste de vérification suivante lors de la configuration de l'authentification utilisateur.

- Pour permettre aux utilisateurs finaux d'accéder aux applications publiées dans Horizon Client sans avoir à s'authentifier, vous devez activer cette fonctionnalité sur l'instance du Serveur de connexion. Pour plus d'informations, consultez les rubriques concernant l'accès sans authentification dans le document *Administration d'Horizon*.
- Pour utiliser l'authentification à deux facteurs, tels que l'authentification RSA SecurID ou RADIUS, avec Horizon Client, vous devez activer la fonctionnalité d'authentification à deux facteurs pour l'instance de Serveur de connexion. À partir de Horizon 7 version 7.11, vous pouvez personnaliser les étiquettes sur la page de connexion d'authentification RADIUS. À partir d'Horizon 7 version 7.12, vous pouvez configurer l'authentification à deux facteurs pour qu'elle se produise après l'expiration d'une session distante. Pour plus d'informations, consultez les rubriques concernant l'authentification à deux facteurs dans le document *Administration d'Horizon*.
- Pour permettre à l'instance du Serveur de connexion d'accepter l'identité de l'utilisateur et les informations d'identification transmises lorsque les utilisateurs sélectionnent **Se connecter en tant qu'utilisateur actuel** dans le menu **Options** dans Horizon Client, activez le paramètre **Autoriser l'ouverture de session en tant qu'utilisateur actuel** pour l'instance du Serveur de connexion. Ce paramètre est disponible dans Horizon 7 version 7.8 et version ultérieure. Pour plus d'informations, reportez-vous au document *Administration d'Horizon*.

  Vous pouvez utiliser les paramètres de stratégie de groupe d'Horizon Client pour configurer la fonctionnalité Se connecter en tant qu'utilisateur actuel, à savoir spécifier une liste d'instances de Serveur de connexion qui peut accepter les informations d'authentification de l'option Se connecter en tant qu'utilisateur actuel. Pour plus d'informations sur ces paramètres côté client, reportez-vous à la section Paramètres de sécurité des objets de stratégie de groupe (GPO) des clients.
- Pour masquer l'URL du serveur dans Horizon Client, activez le paramètre global **Masquer les informations de serveur dans l'interface utilisateur client**. Pour plus d'informations, reportez-vous au document *Administration d'Horizon*.
- Pour masquer le menu déroulant **Domaine** dans Horizon Client, activez le paramètre global **Masquer la liste de domaines dans l'interface utilisateur client**. À partir d'Horizon 7 version 7.8, ce paramètre est activé par défaut. Pour plus d'informations, reportez-vous au document *Administration d'Horizon*.

- Pour envoyer la liste de domaines à Horizon Client, activez-le paramètre global **Envoyer la liste de domaines** dans Horizon Console. Ce paramètre est disponible dans Horizon 7 version 7.8 et version ultérieure et est désactivé par défaut. Les versions antérieures d'Horizon 7 envoient la liste de domaines. Pour plus d'informations, reportez-vous au document *Administration d'Horizon*.

Le tableau suivant montre comment les paramètres globaux **Envoyer la liste de domaines** et **Masquer la liste de domaines dans l'interface utilisateur client** déterminent le mode de connexion des utilisateurs au serveur.

Paramètre Envoyer la liste de domaines	Paramètre Masquer la liste de domaines dans l'interface utilisateur client	Mode de connexion des utilisateurs
Désactivé (par défaut)	Activé	Le menu déroulant **Domaine** est masqué. Les utilisateurs doivent entrer l'une des valeurs suivantes dans la zone de texte **Nom d'utilisateur**. ■ Nom d'utilisateur (non autorisé pour plusieurs domaines) ■ ***domain\username*** ■ ***username@domain.com***
Désactivé (par défaut)	Désactivé	Si un domaine par défaut est configuré sur le client, il s'affiche dans le menu déroulant **Domaine**. Si le client ne connaît pas un domaine par défaut, `*DefaultDomain*` s'affiche dans le menu déroulant **Domaine**. Les utilisateurs doivent entrer l'une des valeurs suivantes dans la zone de texte **Nom d'utilisateur**. ■ Nom d'utilisateur (non autorisé pour plusieurs domaines) ■ ***domain\username*** ■ ***username@domain.com***
Activé	Activé	Le menu déroulant **Domaine** est masqué. Les utilisateurs doivent entrer l'une des valeurs suivantes dans la zone de texte **Nom d'utilisateur**. ■ Nom d'utilisateur (non autorisé pour plusieurs domaines) ■ ***domain\username*** ■ ***username@domain.com***
Activé	Désactivé	Les utilisateurs peuvent entrer un nom d'utilisateur dans la zone de texte **Nom d'utilisateur** et sélectionner un domaine dans le menu déroulant **Domaine**. Ils peuvent également entrer l'une des valeurs suivantes dans la zone de texte **Nom d'utilisateur**. ■ ***domain\username*** ■ ***username@domain.com***

Effacement du dernier nom d'utilisateur utilisé pour se connecter à un serveur

Lorsque des utilisateurs finaux 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 ***domaine**nomutilisateur*** ou ***nomutilisateur*@*domaine***.

Dans un système client Windows, une clé de registre détermine si le dernier nom d'utilisateur est enregistré et affiché dans la zone de texte **Nom d'utilisateur** la prochaine fois qu'un utilisateur se connecte au serveur. Pour éviter d'afficher le dernier nom d'utilisateur dans la zone de texte **Nom d'utilisateur** et ainsi dévoiler des informations sur le domaine, vous devez définir la valeur de la clé de registre `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\dontdisplaylastusername` sur 1 dans le système client Windows.

Pour plus d'informations sur le masquage des informations de sécurité dans Horizon Client, notamment le menu déroulant **Domaine** et les informations sur l'URL de serveur, consultez les rubriques sur les paramètres généraux dans le document *Administration d'Horizon*.

Configurer des options VMware Blast

Vous pouvez configurer des options VMware Blast pour des sessions de poste de travail distant et d'application publiée qui utilisent le protocole d'affichage VMware Blast.

Vous pouvez autoriser le décodage H.264 et le codage vidéo haute performance (HEVC). H.264 est une norme de l'industrie pour la compression vidéo, qui est le processus de conversion d'une vidéo numérique en un format qui occupe moins de capacité lorsqu'il est stocké ou transmis. Lorsque le décodage H.264 est autorisé, vous pouvez également autoriser une meilleure fidélité des couleurs.

La résolution maximale prise en charge, et si le décodage vidéo haute performance est pris en charge, dépend de la capacité du processeur graphique (GPU) sur le client. Un processeur graphique prenant en charge une résolution 4K pour JPEG/PNG peut ne pas prendre en charge une résolution 4K pour H.264. Si une résolution pour H.264 n'est pas prise en charge, Horizon Client utilise JPEG/PNG à la place.

Si votre environnement utilise un serveur proxy, vous pouvez spécifier s'il convient d'autoriser les connexions VMware Blast à un serveur proxy du système d'exploitation.

Pour un serveur proxy SSL, vous devez également configurer la vérification des certificats pour les connexions secondaires via le serveur proxy SSL. Pour plus d'informations, reportez-vous à la section Définition du mode de vérification des certificats dans Horizon Client.

Vous pouvez configurer les options de VMware Blast avant ou après vous être connecté à un serveur.

Conditions préalables

Pour utiliser le codage vidéo haute efficacité (HEVC), Horizon Agent 7.7 ou version ultérieure doit être installé. Pour une meilleure précision des couleurs avec YUV 4:4:4, Horizon Agent 7.11 ou version ultérieure doit être installé. En outre, le système client doit disposer d'un GPU prenant en charge le décodage HEVC.

Le paramètre de stratégie de groupe côté client **Autoriser les connexions Blast à utiliser les paramètres de proxy du système d'exploitation** détermine si les connexions VMware Blast peuvent se connecter via un serveur proxy et si les utilisateurs peuvent modifier le paramètre du serveur proxy de VMware Blast dans l'interface utilisateur d'Horizon Client. Pour plus d'informations, reportez-vous à la section Paramètres généraux des objets de stratégie de groupe (GPO) de clients.

En fonction de la version d'Horizon Agent installée, un administrateur Horizon peut utiliser des paramètres de stratégie de groupe côté agent pour activer ou désactiver les fonctionnalités de VMware Blast, notamment H.264 et la haute précision des couleurs HEVC. Pour plus d'informations, reportez-vous à la section « Paramètres de stratégie VMware Blast » dans le document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Procédure

1. Démarrez Horizon Client.
2. Cliquez sur le bouton **Options** dans le coin supérieur droit de la barre de menus et sélectionnez **Configurer VMware Blast**.

   Si vous êtes connecté à un serveur, vous pouvez cliquer sur l'icône **Paramètres** (engrenage) dans le coin supérieur droit de la fenêtre de sélection des postes de travail et applications et sélectionner **VMware Blast**.
3. Pour autoriser le décodage H.264 dans Horizon Client, cochez la case **Autoriser le décodage H.264**.

   Lorsque cette option est sélectionnée (paramètre par défaut), Horizon Client utilise le décodage H.264 si l'agent prend en charge le codage logiciel ou matériel H.264. Si l'agent ne prend pas en charge le codage logiciel ou matériel H.264, Horizon Client utilise le décodage JPG/PNG (avec Horizon Agent 7.x) ou le décodage de codec Blast (avec Horizon Agent 2006 et version ultérieure). Lorsque cette option est désélectionnée, Horizon Client utilise le décodage JPG/PNG (avec Horizon Agent 7.x) ou le décodage de codec Blast (avec Horizon Agent 2006 et version ultérieure).
4. Pour autoriser une meilleure fidélité des couleurs lorsque le décodage H.264 est autorisé dans Horizon Client, cochez la case **Autoriser la haute précision couleur H (réduit la durée de vie et les performances de la batterie)**.

   Lorsque cette option est sélectionnée, Horizon Client utilise la précision 65536 couleurs si l'agent la prend en charge. La sélection de cette option peut réduire les performances et la durée de vie de la batterie. Cette fonctionnalité est désactivée par défaut.
5. Pour autoriser le décodage vidéo haute performance, cochez la case **Autoriser le décodage vidéo haute performance**.

   Lorsque cette option est sélectionnée, les performances et la qualité d'image sont améliorées si la machine cliente dispose d'un GPU prenant en charge le décodage vidéo haute performance. Cette fonctionnalité est désactivée par défaut.

Si cette option est sélectionnée, mais que la machine cliente n'a pas de GPU prenant en charge le décodage HEVC, Horizon Client utilise plutôt le décodage H.264.

6 Pour autoriser les connexions VMware Blast via un serveur proxy, cochez la case **Autoriser les connexions Blast à utiliser les paramètres de proxy du système d'exploitation**.

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

Résultats

Les modifications seront appliquées la prochaine fois qu'un utilisateur se connectera à une application publiée ou à un poste de travail distant et qu'il sélectionnera le protocole d'affichage VMware Blast. Vos modifications n'ont pas d'incidence sur les sessions VMware Blast existantes.

Utilisation des paramètres proxy d'Internet Explorer

Horizon Client utilise des paramètres proxy configurés dans Internet Explorer.

Contournement des paramètres proxy

Horizon Client utilise les paramètres de contournement de proxy d'Internet Explorer pour contourner les connexions HTTPS vers un hôte du Serveur de connexion, un serveur de sécurité ou un dispositif Unified Access Gateway.

Si le tunnel sécurisé est activé sur l'hôte du Serveur de connexion, le serveur de sécurité ou le dispositif Unified Access Gateway, vous devez utiliser le paramètre de stratégie de groupe `Liste d'adresses de contournement de proxy par tunnel` dans le fichier de modèle d'administration ADM ou ADMX de configuration d'Horizon Client afin de spécifier une liste d'adresses pour contourner la connexion par tunnel. Le serveur proxy n'est pas utilisé pour ces adresses. Utilisez un point-virgule (;) pour séparer plusieurs entrées. Ce paramètre de stratégie de groupe crée la clé de registre suivante :

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\VMware, Inc.\VMware VDM\Client\TunnelProxyBypass
```

Vous ne pouvez pas utiliser ce paramètre de stratégie de groupe pour les connexions directes. Si l'application du paramètre de stratégie de groupe ne fonctionne pas comme prévu, essayez de contourner le proxy pour les adresses locales. Pour plus d'informations, consultez https://blogs.msdn.microsoft.com/askie/2015/10/12/how-to-configure-proxy-settings-for-ie10-and-ie11-as-iem-is-not-available/.

Basculement de proxy

Horizon Client prend en charge le basculement de proxy avec le paramètre **Utiliser un script de configuration automatique** sous **Configuration automatique** dans **Options Internet > Connexions > Paramètres de réseau local** dans Internet Explorer. Pour utiliser ce paramètre, vous devez créer un script de configuration automatique qui renvoie plusieurs serveurs proxy.

Configurer le partage de données d'Horizon Client

Si un administrateur Horizon a choisi de participer au programme d'amélioration du produit (CEIP) de VMware, VMware recueille et reçoit des données anonymes des systèmes clients via le Serveur de connexion. Vous pouvez déterminer si vous souhaitez partager ces données client avec le Serveur de connexion.

Pour plus d'informations sur la configuration d'Horizon afin de participer au programme CEIP, reportez-vous au document *Administration d'Horizon*.

Le partage de données est activé par défaut dans Horizon Client. Vous devez configurer le paramètre de partage de données avant de vous connecter à un serveur. Le paramètre est appliqué à tous les serveurs. Vous ne pouvez pas modifier le paramètre de partage de données Horizon Client après vous être connecté à un serveur.

Vous pouvez utiliser le paramètre de stratégie de groupe **Autoriser le partage de données** pour activer ou désactiver le partage de données et empêcher les utilisateurs de modifier le paramètre dans l'interface utilisateur de Horizon Client. Pour plus d'informations, reportez-vous à la section Paramètres généraux des objets de stratégie de groupe (GPO) de clients.

Procédure

1. Cliquez sur le bouton **Options** dans le coin supérieur droit et sélectionnez **Autoriser le partage de données**.
2. Définissez le mode de partage des données sur **Activé** ou sur **Désactivé** et cliquez sur **OK**.

Données Horizon Client collectées par VMware

Si un administrateur Horizon a choisi de participer au programme d'amélioration du produit et que le partage de données est activé sur le système client, VMware collecte des données sur le système client.

VMware collecte des données sur les systèmes clients afin de hiérarchiser la compatibilité matérielle et logicielle. Si l'administrateur Horizon a choisi de participer au programme d'amélioration du produit, VMware collecte des données anonymes sur votre déploiement afin de mieux répondre aux exigences des clients. VMware ne collecte pas les données d'identification de votre organisation. Les informations d'Horizon Client sont envoyées d'abord à l'instance du Serveur de connexion, puis à VMware, avec des données sur le Serveur de connexion, les pools de postes de travail et les postes de travail distants.

Les informations sont chiffrées lorsqu'elles sont transmises à l'instance du Serveur de connexion. Les informations sur le système client sont journalisées non chiffrées dans un répertoire spécifique à l'utilisateur. Les journaux ne contiennent aucune information d'identification personnelle.

L'administrateur Horizon peut choisir de participer ou non au programme d'amélioration du produit VMware lors de l'installation du Serveur de connexion ou en définissant une option dans Horizon Console après l'installation.

Tableau 1-1. Données collectées depuis Horizon Client pour le programme d'amélioration du produit

Description	Ce champ reste-t-il anonyme ?
Entreprise ayant produit l'application Horizon Client	Non
Nom du produit	Non
Version du produit client	Non
Architecture binaire du client	Non
Nom du build du client	Non
Système d'exploitation hôte	Non
Noyau du système d'exploitation hôte	Non
Architecture du système d'exploitation hôte	Non
Modèle du système hôte	Non
Processeur du système hôte	Non
Nombre de cœurs dans le processeur du système hôte	Non
Mo de mémoire sur le système hôte	Non
Nombre de périphériques USB connectés	Non
Nombre maximal de connexions de périphériques USB simultanées	Non
ID de fournisseur de périphériques USB	Non
ID de produit de périphérique USB	Non
Famille de périphériques USB	Non
Nombre d'utilisations du périphérique USB	Non

Installation d'Horizon Client pour Windows

2

Vous pouvez obtenir le programme d'installation d'Horizon Client pour Windows sur le site Web de VMware ou depuis une page d'accès Web fournie par le Serveur de connexion. Vous pouvez définir différentes options de démarrage pour les utilisateurs finaux après l'installation d'Horizon Client.

Ce chapitre contient les rubriques suivantes :

- Activation du mode FIPS sur le système d'exploitation client Windows
- Activation de la sélection automatique du protocole Internet
- Installer Horizon Client pour Windows
- Installation d'Horizon Client à partir de la ligne de commande
- Vérifiez l'installation de Redirection de contenu URL
- Mettre à jour Horizon Client en ligne

Activation du mode FIPS sur le système d'exploitation client Windows

Si vous prévoyez d'installer Horizon Client avec un chiffrement compatible FIPS (Federal Information Processing Standard), vous devez activer le mode FIPS sur le système d'exploitation client avant d'exécuter le programme d'installation d'Horizon Client.

Lorsque le mode FIPS est activé dans le système d'exploitation client, les applications n'utilisent que des algorithmes de chiffrement compatibles avec FIPS-140 et conformes aux modes d'opération approuvés par FIPS. Vous pouvez activer le mode FIPS en activant un paramètre de sécurité spécifique, dans la stratégie de sécurité locale ou dans le cadre de la stratégie de groupe, ou en modifiant une clé de registre Windows.

Pour plus d'informations sur la conformité FIPS, consultez le document *Installation d'Horizon*.

Définition de la propriété de configuration FIPS

Pour activer le mode FIPS sur le système d'exploitation client, vous pouvez utiliser un paramètre de stratégie de groupe Windows ou un paramètre de registre Windows pour l'ordinateur client.

- Pour utiliser le paramètre de stratégie de groupe, ouvrez l'éditeur de stratégie de groupe, accédez à `Configuration ordinateur\Paramètres Windows\Paramètres de sécurité\Stratégies locales\Options de sécurité` et activez le paramètre **Chiffrement système : utilisez des algorithmes compatibles FIPS pour le chiffrement, le hachage et la signature**.
- Pour utiliser le registre Windows, accédez à `HKLM\System\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy\Enabled` et définissez **Activé** sur 1.

Pour plus d'informations sur le mode FIPS, consultez https://support.microsoft.com/en-us/kb/811833.

Important Si vous n'activez pas le mode FIPS avant d'exécuter le programme d'installation d'Horizon Client, l'option du programme d'installation pour utiliser le chiffrement compatible FIPS ne s'affiche pas lors d'une installation personnalisée. Le chiffrement compatible FIPS n'est pas activé lors d'une installation classique. Si vous installez Horizon Client sans l'option de chiffrement compatible FIPS et que vous décidez ultérieurement d'utiliser l'option, vous devez désinstaller le client, activer le mode FIPS sur le système d'exploitation client et exécuter de nouveau le programme d'installation d'Horizon Client.

Activation de la sélection automatique du protocole Internet

Lorsque vous effectuez une installation personnalisée d'Horizon Client, vous pouvez activer la sélection automatique du protocole Internet. Avec la sélection automatique, Horizon Client vérifie le réseau en cours et se connecte automatiquement via IPv4 ou IPv6.

Lorsque la sélection automatique est activée, les fonctionnalités suivantes sont prises en charge avec Unified Access Gateway 3.3 et version ultérieure avec le protocole d'affichage VMware Blast.

- Se connecter en tant qu'utilisateur actuel
- Sortie audio
- Collecte de données du Programme d'amélioration du produit
- Impression virtuelle
- VMware Integrated Printing (requiert Horizon 7 version 7.7 ou version ultérieure)
- Redirection multimédia HTML5
- Vidéo VMware
- Redirection USB

- Audio/Vidéo en temps réel (RTAV)

Installer Horizon Client pour Windows

Vous pouvez exécuter un fichier du programme d'installation Windows pour installer tous les composants d'Horizon Client.

Cette procédure décrit comment installer Horizon Client à l'aide d'un assistant d'installation interactive. Pour installer Horizon Client à partir de la ligne de commande, reportez-vous à la section Installation d'Horizon Client à partir de la ligne de commande. Pour installer la fonctionnalité Redirection de contenu URL, vous devez exécuter le programme d'installation à partir de la ligne de commande.

Note Vous pouvez installer Horizon Client sur la machine virtuelle du poste de travail distant. Les entreprises peuvent utiliser cette stratégie d'installation si leurs utilisateurs finaux accèdent à des applications publiées à partir de périphériques de client léger Windows.

Conditions préalables

- Vérifiez que le système client utilise un système d'exploitation pris en charge. Reportez-vous à la section Configuration système requise pour les systèmes clients Windows.
- Vérifiez que vous disposez de l'URL d'accès à une page de téléchargement contenant le programme d'installation d'Horizon Client. Il peut s'agir de l'URL de la page de téléchargements de VMware à l'adresse http://www.vmware.com/go/viewclients ou de l'URL d'une instance du Serveur de connexion.
- Vérifiez que vous pouvez ouvrir une session en tant qu'administrateur sur le système client.
- vérifiez que les contrôleurs de domaine disposent des derniers correctifs, d'un espace disque libre suffisant et peuvent communiquer entre eux.
- Si vous prévoyez d'installer Horizon Client avec la cryptographie compatible FIPS, activez le mode FIPS dans le système d'exploitation client. Reportez-vous à la section Activation du mode FIPS sur le système d'exploitation client Windows.
- Si vous prévoyez de sélectionner le protocole IPv6 ou d'activer la sélection automatique du protocole Internet, consultez le document *Installation d'Horizon* pour plus d'informations sur les fonctionnalités qui ne sont pas disponibles dans un environnement IPv6.
- Si vous prévoyez d'activer la sélection automatique du protocole Internet, reportez-vous à la section Activation de la sélection automatique du protocole Internet pour plus d'informations sur les fonctionnalités prises en charge.
- Si vous prévoyez d'installer le composant **Redirection USB**, procédez comme suit :
  - Déterminez si la personne qui utilise le périphérique client est autorisée à accéder à des périphériques USB connectés en local depuis un poste de travail distant. Si l'accès n'est pas autorisé, n'installez pas le composant **Redirection USB** ou bien installez le composant et désactivez-le en utilisant un paramètre de stratégie de groupe. Si vous utilisez une

stratégie de groupe pour désactiver la redirection USB, vous n'avez pas besoin de réinstaller Horizon Client si vous décidez ultérieurement d'activer la redirection USB pour un client. Pour plus d'informations, reportez-vous à la section Paramètres de définition de scripts des objets de stratégie de groupe (GPO) des clients.

- Vérifiez que la fonctionnalité Mise à jour automatique Windows n'est pas désactivée sur l'ordinateur client.

- Décidez s'il convient ou non d'utiliser la fonctionnalité qui permet à des utilisateurs finaux d'ouvrir une session sur Horizon Client et sur leur poste de travail virtuel en tant qu'utilisateur actuellement connecté. Les informations d'identification que l'utilisateur a saisies lors de l'ouverture de session sur le système client sont transmises à l'instance du Serveur de connexion, puis au poste de travail distant. Certains systèmes d'exploitation client ne prennent pas cette fonction en charge.
- Si vous ne voulez pas que les utilisateurs finaux aient à fournir le nom de domaine complet (FQDN) de l'instance du Serveur de connexion, déterminez le FQDN pour que vous puissiez le fournir lors de l'installation.

Procédure

1. Connectez-vous au système client comme administrateur.
2. Accédez à la page de téléchargements de VMware à l'adresse http://www.vmware.com/go/viewclients.
3. Téléchargez le fichier d'installation, par exemple, `VMware-Horizon-Client-`*`YYMM`*`-`*`y.y.y`*`-`*`xxxxxx`*`.exe`.

   YYMM est le numéro de version marketing, *y.y.y* est le numéro de version interne et *xxxxxx* est le numéro de build.
4. Double-cliquez sur le fichier du programme d'installation pour commencer l'installation.

5 Sélectionnez le type d'installation et suivez les invites.

Option	Action
Installation classique	Cliquez sur **Accepter et installer**. Le programme d'installation configure le client pour qu'il utilise le protocole Internet IPv4 et installe les fonctionnalités suivantes. ■ Redirection USB ■ Connectez-vous en tant qu'utilisateur actuel, notamment en affichant l'option **Se connecter en tant qu'utilisateur actuel**. ■ Pack de virtualisation pour Skype Entreprise ■ Prise en charge de la redirection multimédia HTML5 et de la redirection de navigateur ■ Optimisation des supports pour Microsoft Teams
Installation personnalisée	Cliquez sur **Personnaliser l'installation** et sélectionnez les fonctions à installer. Vous devez sélectionner cette option pour installer les fonctionnalités suivantes. ■ Spécifier un emplacement d'installation autre que celui par défaut. ■ Utilisez le protocole Internet IPv6 ou la sélection automatique. Si vous activez la sélection automatique, Horizon Client vérifie le réseau en cours et se connecte automatiquement via IPv4 ou IPv6. ■ Définissez le comportement de connexion par défaut sur **Se connecter en tant qu'utilisateur actuel**. ■ Spécifiez une instance du Serveur de connexion par défaut. ■ Activer la cryptographie compatible FIPS. Les options d'installation personnalisée du chiffrement compatible FIPS sont disponibles dans le programme d'installation uniquement si le mode FIPS est activé sur le système d'exploitation client.

Résultats

Certaines fonctionnalités nécessitent que vous redémarriez le système client.

Le programme d'installation installe les services Windows, notamment VMware Horizon Client (`horizon_client_service`) et VMware USB Arbitration Service (`VMUSBArbService`).

Étape suivante

Démarrez Horizon Client et vérifiez que vous pouvez ouvrir une session sur l'application publiée ou le poste de travail distant correct. Reportez-vous à la section Se connecter à un poste de travail distant ou à une application publiée.

Installation d'Horizon Client à partir de la ligne de commande

Vous pouvez installer Horizon Client en saisissant le nom de fichier du programme d'installation, les commandes d'installation et les propriétés d'installation dans la ligne de commande.

Lorsque vous installez Horizon Client à partir de la ligne de commande, vous pouvez effectuer une installation silencieuse. L'installation silencieuse vous permet de déployer efficacement Horizon Client dans une entreprise de grande taille.

Commandes d'installation d'Horizon Client

Lorsque vous installez Horizon Client à partir de la ligne de commande, vous pouvez spécifier certaines commandes d'installation.

Le tableau suivant décrit les commandes d'installation d'Horizon Client.

Tableau 2-1. Commandes d'installation d'Horizon Client

vdmadmin	Description
`/?` ou `/help`	Répertorie les propriétés et les commandes d'installation d'Horizon Client.
`/silent`	Installe Horizon Client en mode silencieux. Vous n'avez pas besoin de répondre aux invites de l'Assistant.
`/install`	Installe Horizon Client de manière interactive. Vous devez répondre aux invites de l'Assistant.
`/uninstall`	Désinstalle Horizon Client.
`/repair`	Répare Horizon Client.
`/norestart`	Supprime tous les redémarrages et les invites de redémarrage au cours du processus d'installation.
`/x /extract`	Extrait les modules du programme d'installation dans le répertoire `TEMP %`.
`/l` ou `/log`	Spécifie un dossier et un mode d'attribution de nom pour les fichiers journaux d'installation. Par exemple, si vous spécifiez la commande suivante, le programme d'installation d'Horizon Client crée des fichiers journaux qui ont le préfixe `Test` dans le dossier nommé `C:\Temp`. `/log "C:\Temp\Test"`

Propriétés d'installation d'Horizon Client

Lorsque vous installez Horizon Clientà partir de la ligne de commande, vous pouvez spécifier certaines propriétés d'installation.

Le tableau suivant décrit les propriétés d'installation d'Horizon Client.

Tableau 2-2. Propriétés d'installation d'Horizon Client

Propriété	Description	Valeur par défaut
INSTALLDIR	Chemin d'accès et dossier dans lequel Horizon Client est installé. Par exemple : `INSTALLDIR=""D:\abc\my folder""` Les guillemets délimitant le chemin permettent au programme d'installation d'interpréter l'espace comme étant une partie valide du chemin.	`%ProgramFiles%VMware\VMware Horizon View Client`
VDM_IP_PROTOCOL_USAGE	Version IP (Protocole Internet) que les composants Horizon Client utilisent pour la communication. Les valeurs valides sont les suivantes : ■ IPv4 ■ IPv6 ■ Double Si vous spécifiez Double, Horizon Client vérifie le réseau actuel et se connecte automatiquement via IPv4 ou IPv6.	IPv4
VDM_FIPS_ENABLED	Détermine s'il faut installer Horizon Client avec la cryptographie compatible FIPS. La valeur 1 installe Horizon Client avec un chiffrement compatible FIPS. La valeur 0 installe Horizon Client sans chiffrement compatible FIPS. **Note** Avant de définir cette propriété sur 1, vous devez activer le mode FIPS sur le système d'exploitation client Windows. Reportez-vous à la section Activation du mode FIPS sur le système d'exploitation client Windows.	0
VDM_SERVER	Nom de domaine complet (FQDN) de l'instance du Serveur de connexion à laquelle les utilisateurs d'Horizon Client se connectent par défaut. Par exemple : `VDM_Server=cs1.companydomain.com` Si vous configurez cette propriété, les utilisateurs d'Horizon Client n'ont pas à fournir ce nom de domaine complet (FQDN).	Aucun
LOGINASCURRENTUSER_DISPLAY	Détermine si **Se connecter en tant qu'utilisateur actuel** s'affiche dans le menu **Options** de la barre de menus Horizon Client. Les valeurs valides sont 1 (activé) ou 0 (désactivé).	1

Tableau 2-2. Propriétés d'installation d'Horizon Client (suite)

Propriété	Description	Valeur par défaut
LOGINASCURRENTUSER_DEFAULT	Détermine si **Se connecter en tant qu'utilisateur actuel** est sélectionné par défaut dans le menu **Options** de la barre de menus Horizon Client. Les valeurs valides sont 1 (activé) et 0 (désactivé). Lorsque l'option Se connecter en tant qu'utilisateur actuel est le comportement de connexion par défaut, l'identité et les informations d'identification que l'utilisateur a fournies lors de la connexion au système client sont transmises à l'instance du Serveur de connexion, puis au poste de travail distant. Lorsque l'option Se connecter en tant qu'utilisateur actuel n'est pas le comportement de connexion par défaut, les utilisateurs doivent fournir leur identité et leurs informations d'identification plusieurs fois avant de pouvoir accéder à une application ou un poste de travail distant.	0
ADDLOCAL	Spécifie les fonctionnalités à installer. Les valeurs valides sont les suivantes : ■ ALL : installe toutes les fonctionnalités disponibles, à l'exception de Redirection de contenu URL. ■ TSSO : installe la fonctionnalité Se connecter en tant qu'utilisateur actuel. ■ USB : installe la fonctionnalité Redirection USB. Pour spécifier des fonctionnalités individuelles, entrez une liste de noms de fonctionnalités séparés par des virgules. Ne laissez pas d'espaces entre les noms. Par exemple, pour installer Horizon Client avec la fonctionnalité Redirection USB, mais sans la fonctionnalité Se connecter en tant qu'utilisateur actuel, tapez la commande suivante : `VMware-Horizon-Client-y.y.y-xxxxxx.exe ADDLOCAL=USB`	Aucun
INSTALL_SFB	Détermine si le pack de virtualisation VMware pour Skype entreprise est installé. La fonctionnalité sera installée si la valeur est égale à 1. La fonctionnalité ne sera pas installée si la valeur est égale à 0.	1

Tableau 2-2. Propriétés d'installation d'Horizon Client (suite)

Propriété	Description	Valeur par défaut
INSTALL_HTML5MMR	Détermine si la fonctionnalité Prise en charge de la redirection multimédia HTML5 et de la redirection de navigateur est installée. La fonctionnalité sera installée si la valeur est égale à 1. La fonctionnalité ne sera pas installée si la valeur est égale à 0.	1
REMOVE	Spécifie les fonctionnalités à ne pas installer. Les valeurs valides sont les suivantes : ■ ThinPrint : n'installe pas la fonctionnalité d'impression virtuelle. ■ Scanner : n'installe pas la fonctionnalité de redirection de scanner. ■ FolderRedirection : n'installe pas la fonctionnalité de redirection de dossier. ■ SerialPort : n'installe pas la fonctionnalité de redirection de port série. Pour spécifier plusieurs fonctionnalités, entrez une liste de noms de fonctionnalités séparés par des virgules. Ne laissez pas d'espaces entre les noms. Par exemple, la commande suivante n'installe pas les fonctionnalités d'impression virtuelle et de redirection de scanner : VMware-Horizon-Client-*y.y.y*-*xxxxxx*.exe REMOVE=ThinPrint,Scanner	Aucun
DESKTOP_SHORTCUT	Détermine s'il faut créer un raccourci Bureau pour Horizon Client. La valeur 0 ne crée pas un raccourci Bureau. La valeur 1 crée un raccourci Bureau.	1
STARTMENU_SHORTCUT	Détermine s'il faut créer un raccourci de menu Démarrer pour Horizon Client. La valeur 0 ne crée pas un raccourci de menu Démarrer. La valeur 1 crée un raccourci de menu Démarrer.	1

Tableau 2-2. Propriétés d'installation d'Horizon Client (suite)

Propriété	Description	Valeur par défaut
URL_FILTERING_ENABLED	Détermine si la fonctionnalité de redirection de contenu URL est installée. La fonctionnalité sera installée si la valeur est égale à 1. La fonctionnalité ne sera pas installée si la valeur est égale à 0. Lorsque vous affectez 1 à cette propriété dans une installation interactive, la case à cocher **Redirection de contenu URL** s'affiche sous Fonctionnalités supplémentaires dans la boîte de dialogue d'installation personnalisée et est sélectionnée par défaut. La case à cocher ne s'affiche pas, sauf si vous affectez 1 à cette propriété. **Note** La propriété ADDLOCAL=ALL n'inclut pas la fonctionnalité Redirection de contenu URL.	0
AUTO_UPDATE_ENABLED	Détermine si la fonctionnalité de mise à jour en ligne est activée. La fonctionnalité est activée si la valeur est égale à 1. La fonctionnalité est désactivée si la valeur est égale à 0. Pour plus d'informations, reportez-vous à la section Mettre à jour Horizon Client en ligne.	1
INSTALL_TEAMS_REDIRECTION	Détermine si la fonctionnalité Optimisation des supports pour Microsoft Teams est activée. La fonctionnalité est activée si la valeur est égale à 1. La fonctionnalité est désactivée si la valeur est égale à 0. Pour plus d'informations sur cette fonctionnalité, consultez le document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.	1

Installation d'Horizon Client à partir de la ligne de commande

Vous pouvez installer Horizon Client à partir de la ligne de commande en tapant le nom de fichier du programme d'installation et en spécifiant des propriétés et des commandes d'installation. Vous pouvez installer Horizon Clienten mode silencieux à partir de la ligne de commande.

Conditions préalables

- Vérifiez que le système client utilise un système d'exploitation pris en charge. Reportez-vous à la section Configuration système requise pour les systèmes clients Windows.
- Vérifiez que vous pouvez ouvrir une session en tant qu'administrateur sur le système client.
- vérifiez que les contrôleurs de domaine disposent des derniers correctifs, d'un espace disque libre suffisant et peuvent communiquer entre eux.

- Si vous prévoyez d'installer Horizon Client avec la cryptographie compatible FIPS, activez le mode FIPS dans le système d'exploitation client. Reportez-vous à la section Activation du mode FIPS sur le système d'exploitation client Windows.
- Décidez s'il convient ou non d'utiliser la fonctionnalité qui permet à des utilisateurs finaux d'ouvrir une session sur Horizon Client et sur leur poste de travail virtuel en tant qu'utilisateur actuellement connecté. Les informations d'identification que l'utilisateur a saisies lors de l'ouverture de session sur le système client sont transmises à l'instance du Serveur de connexion, puis au poste de travail distant. Certains systèmes d'exploitation client ne prennent pas cette fonction en charge.
- Familiarisez-vous avec les commandes d'installation d'Horizon Client. Reportez-vous à la section Commandes d'installation d'Horizon Client.
- Familiarisez-vous avec les propriétés d'installation d'Horizon Client. Reportez-vous à la section Propriétés d'installation d'Horizon Client.
- Déterminez si vous voulez autoriser les utilisateurs finaux à accéder à des périphériques USB connectés en local à partir de leurs postes de travail distants. Si ce n'est pas le cas, définissez la propriété d'installation `ADDLOCAL` sur la liste des fonctionnalités et omettez la fonctionnalité USB. Pour plus d'informations, reportez-vous à la section Propriétés d'installation d'Horizon Client.
- Si vous ne voulez pas que les utilisateurs finaux aient à fournir le nom de domaine complet (FQDN) de l'instance du Serveur de connexion, déterminez le FQDN pour que vous puissiez le fournir lors de l'installation.

Procédure

1. Connectez-vous au système client comme administrateur.
2. Accédez à la page de téléchargements de VMware à l'adresse http://www.vmware.com/go/viewclients.
3. Téléchargez le fichier d'installation d'Horizon Client, par exemple, `VMware-Horizon-Client-`*`YYMM`*`-`*`y.y.y`*`-`*`xxxxxx`*`.exe`.

   YYMM est le numéro de version marketing, *y.y.y* est le numéro de version interne et *xxxxxx* est le numéro de build.
4. Ouvrez une invite de commande sur l'ordinateur client Windows.
5. Entrez le nom de fichier du programme d'installation, les commandes d'installation et les propriétés d'installation sur une seule ligne.

   `VMware-Horizon-Client-`*`YYMM`*`-`*`y.y.y`*`-`*`xxxxxx`*`.exe [`*`commands`*`] [`*`properties`*`]`

Résultats

Le programme d'installation installe Horizon Client selon les commandes d'installation et les propriétés que vous spécifiez. Si vous spécifiez la commande d'installation `/silent`, les invites de l'Assistant ne s'affichent pas.

Le programme d'installation installe les services Windows, notamment VMware Horizon Client (`horizon_client_service`) et VMware USB Arbitration Service (`VMUSBArbService`).

Exemple : Exemples de commandes d'installation

La commande suivante installe Horizon Client de manière interactive et active la fonctionnalité Redirection de contenu URL.

```
VMware-Horizon-Client-YYMM-y.y.y-xxxxxx.exe URL_FILTERING_ENABLED=1
```

La commande suivante installe Horizon Client en mode silencieux et supprime tous les redémarrages et les invites de redémarrage au cours du processus d'installation.

```
VMware-Horizon-Client-YYMM-y.y.y-xxxxxx.exe /silent /norestart
```

Étape suivante

Si vous avez activé la fonctionnalité Redirection de contenu URL lorsque vous avez installé Horizon Client, vérifiez que la fonctionnalité est installée. Reportez-vous à la section Vérifiez l'installation de Redirection de contenu URL.

Démarrez Horizon Client et vérifiez que vous pouvez ouvrir une session sur l'application publiée ou le poste de travail distant correct. Reportez-vous à la section Se connecter à un poste de travail distant ou à une application publiée.

Vérifiez l'installation de Redirection de contenu URL

Si vous avez activé la fonctionnalité Redirection de contenu URL lorsque vous avez installé Horizon Client, vérifiez que la fonctionnalité a été installée.

Conditions préalables

Spécifiez la propriété d'installation `URL_FILTERING_ENABLED=1` lorsque vous installez Horizon Client. Reportez-vous à la section Installation d'Horizon Client à partir de la ligne de commande.

Procédure

1. Connectez-vous à la machine cliente.
2. Vérifiez que les fichiers `vmware-url-protocol-launch-helper.exe` et `vmware-url-filtering-plugin` sont installés dans le répertoire `%PROGRAMFILES%\VMware\VMware Horizon View Client\`.
3. Vérifiez que le plug-in de filtrage d'URL de VMware Horizon View est installé et activé dans Internet Explorer.

Mettre à jour Horizon Client en ligne

Vous pouvez mettre Horizon Client à jour en ligne.

Par défaut, un point rouge apparaît dans le menu **Options** (avant de vous connecter à un serveur) et sur le bouton **Aide** (après vous être connecté à un serveur) pour indiquer qu'une nouvelle version d'Horizon Client est disponible.

Au cours du processus de mise à jour, par défaut, vous pouvez cocher ou décocher la case **Rechercher les mises à jour et afficher la notification de badge** pour spécifier si Horizon Client doit rechercher automatiquement les mises à jour et afficher la nouvelle notification de version.

Vous pouvez contrôler le comportement de la fonctionnalité de mise à jour en ligne en configurant les paramètres de stratégie de groupe suivants.

- **Activer les mises à jour en ligne d'Horizon Client**, qui active ou désactive la fonctionnalité de mise à jour en ligne.
- **URL de la mise à jour en ligne d'Horizon Client**, qui spécifie une autre URL à partir de laquelle Horizon Client peut récupérer les mises à jour.
- **Rechercher automatiquement les mises à jour**, qui contrôle la case **Rechercher les mises à jour et afficher la notification de badge**.
- **Mettre à jour le message contextuel**, qui contrôle la case **Afficher le message contextuel en cas de mise à jour**. La case **Afficher le message contextuel en cas de mise à jour** prend effet uniquement si la case **Rechercher les mises à jour et afficher la notification de badge** est cochée.
- **Autoriser l'utilisateur à ignorer une mise à jour d'Horizon Client**, qui contrôle le bouton **Ignorer**.

Pour plus d'informations sur ces paramètres de stratégie de groupe, reportez-vous à la section Paramètres généraux des objets de stratégie de groupe (GPO) de clients.

Vous pouvez également désactiver la fonctionnalité de mise à jour en ligne en définissant la propriété `AUTO_UPDATE_ENABLED` sur 0 lorsque vous installez Horizon Client à partir de la ligne de commande. Pour plus d'informations, reportez-vous à la section Propriétés d'installation d'Horizon Client.

Conditions préalables

- Enregistrez votre travail avant d'effectuer la mise à jour d'Horizon Client. La mise à jour peut initier un redémarrage système.
- Vérifiez que vous pouvez ouvrir une session en tant qu'administrateur sur le système client.

Procédure

1. Connectez-vous au système client comme administrateur.

2 Démarrez Horizon Client et cliquez sur **Mises à jour logicielles**.

Option	Action
Avant de vous connecter à un serveur	Cliquez sur **Options > Mises à jour du logiciel**.
Après vous être connecté à un serveur	Cliquez sur **Aide > Mises à jour logicielles**.

3 Pour rechercher les mises à jour disponibles, cliquez sur **Rechercher les mises à jour**.

Horizon Client indique si une mise à jour est disponible.

4 Pour commencer le processus de mise à jour si une nouvelle version est disponible, cliquez sur **Télécharger et installer**.

Vous pouvez également cliquer sur **Ignorer** (le cas échéant) ou sur **Me le rappeler ultérieurement** pour installer la mise à jour à un autre moment. Si vous cliquez sur **Ignorer**, vous ne voyez pas d'autres notifications de mise à jour tant que la version suivante d'Horizon Client n'est pas disponible. Vous pouvez toujours cliquer sur **Mises à jour logicielles** pour rechercher manuellement une mise à jour.

5 Pour installer la mise à jour après qu'Horizon Client l'a téléchargée, cliquez sur **OK**.

L'assistant d'installation interactive d'Horizon Client s'ouvre.

Configuration d'Horizon Client pour les utilisateurs finaux

3

La configuration d'Horizon Client pour les utilisateurs finaux peut impliquer la configuration des URI pour démarrer Horizon Client, la configuration du mode de vérification des certificats, la définition d'options TLS avancées, la personnalisation des menus d'Horizon Client et l'utilisation de stratégies de groupe pour configurer des paramètres personnalisés.

Ce chapitre contient les rubriques suivantes :

- Paramètres de configuration communs
- Utilisation d'URI pour configurer Horizon Client
- Définition du mode de vérification des certificats dans Horizon Client
- Configuration du mode de vérification des certificats pour les utilisateurs finaux
- Configuration des options TLS avancées
- Personnalisation des menus d'Horizon Client
- Personnalisation des messages d'erreur d'Horizon Client
- Configuration de la gestion des événements du curseur
- Utilisation de paramètres de stratégie de groupe pour configurer Horizon Client
- Exécution d'Horizon Client depuis la ligne de commande
- Utilisation du Registre Windows pour configurer Horizon Client

Paramètres de configuration communs

Horizon Client fournit plusieurs mécanismes de configuration permettant de simplifier les processus de connexion et de sélection d'un poste de travail pour les utilisateurs finaux et de renforcer les stratégies de sécurité.

Le tableau suivant ne présente qu'une partie des paramètres de configuration que vous pouvez définir de plusieurs manières.

Tableau 3-1. Paramètres de configuration communs

Paramètre	Mécanismes de configuration
Adresse du serveur	URI, Stratégie de groupe, Ligne de commande, Registre Windows
Nom d'utilisateur Active Directory	URI, Stratégie de groupe, Ligne de commande, Registre Windows
Nom de domaine	URI, Stratégie de groupe, Ligne de commande, Registre Windows
Nom d'affichage du poste de travail distant	URI, Stratégie de groupe, Ligne de commande
Taille de fenêtre	URI, Stratégie de groupe, Ligne de commande
Protocole d'affichage	URI, Ligne de commande
Configuration de la vérification des certificats	Stratégie de groupe, Registre Windows
Configuration des protocoles et des algorithmes de chiffrement TLS	Stratégie de groupe, Registre Windows

Utilisation d'URI pour configurer Horizon Client

Vous pouvez utiliser des identifiants uniformes de ressource (URI) pour créer une page Web ou des liens d'e-mail sur lesquels les utilisateurs finaux peuvent cliquer pour démarrer Horizon Client, se connecter à un serveur ou ouvrir un poste de travail distant ou une application publiée.

Vous pouvez créer ces liens en construisant des URI qui fournissent une partie ou l'intégralité des informations suivantes, afin que les utilisateurs finaux n'aient pas à les fournir.

- Adresse du serveur
- Numéro de port du serveur
- Nom d'utilisateur Active Directory
- Nom d'utilisateur RADIUS ou RSA SecurID, s'il est différent du nom d'utilisateur Active Directory
- Nom de domaine
- Nom d'affichage du poste de travail distant ou de l'application publiée
- Taille de fenêtre
- Actions incluant la réinitialisation, la déconnexion et le démarrage d'une session
- Protocole d'affichage
- Options pour la redirection des périphériques USB

Pour construire un URI, vous pouvez utiliser le schéma d'URI `vmware-view` avec des éléments de chemin et de requête propres à Horizon Client.

Pour utiliser des URI pour démarrer Horizon Client, Horizon Client doit déjà être installé sur les ordinateurs clients.

Syntaxe pour la création d'URI vmware-view

La syntaxe d'UIR comprend le schéma d'URI `vmware-view`, un chemin d'accès spécifiant le poste de travail distant ou l'application publiée et, en option, une requête permettant de spécifier les actions ou les options de configuration.

Spécification d'URI

Utilisez la syntaxe suivante pour créer des URI pour démarrer Horizon Client.

```
vmware-view://[authority-part][/path-part][?query-part]
```

Le seul élément requis est le schéma d'URI, `vmware-view`. Étant donné que le nom du schéma est sensible à la casse pour certaines versions de certains systèmes d'exploitation clients, tapez `vmware-view`.

Important Pour tous les éléments, les caractères non ASCII doivent d'abord être encodés en UTF-8 [STD63], puis chaque octet de la séquence UTF-8 correspondante doit être codé en pourcentage pour être représenté en tant que caractères URI.

Pour plus d'informations sur l'encodage de caractères ASCII, consultez la référence d'encodage d'URL sur http://www.utf8-chartable.de/.

authority-part

Adresse du serveur et, éventuellement, un nom d'utilisateur, un numéro de port non défini par défaut, ou bien les deux. Les traits de soulignement (_) ne sont pas pris en charge dans les noms de serveur. Les noms de serveur doivent être conformes à la syntaxe DNS.

Pour spécifier un nom d'utilisateur, utilisez la syntaxe suivante.

```
user1@server-address
```

Vous ne pouvez pas spécifier d'adresse UPN, ce qui inclut le domaine. Pour spécifier le domaine, vous pouvez utiliser la partie de requête `domainName` de l'URI.

Pour spécifier un numéro de port, utilisez la syntaxe suivante.

```
server-address:port-number
```

path-part

Nom d'affichage du poste de travail distant ou de l'application publiée. Le nom d'affichage est spécifié dans Horizon Console lorsque le pool de postes de travail ou le pool d'applications est créé. Si le nom d'affichage contient un espace, utilisez le mécanisme de codage **%20** pour représenter l'espace.

Vous pouvez également spécifier un ID de poste de travail ou d'application, qui est une chaîne de chemin d'accès comportant l'ID de pool de postes de travail ou d'application. Pour trouver un ID de poste de travail ou d'application, ouvrez ADSI Edit sur l'hôte du serveur de connexion, accédez à `DC=vdi,dc=vmware,dc=int` et sélectionnez le nœud `OU=Applications`. Tous les pools de postes de travail et d'applications sont répertoriés. L'attribut `distinguishedName` spécifie la valeur de l'ID. Vous devez coder la valeur de l'ID avant de la spécifier dans un URI, par exemple, `cn%3Dwin7-32%2Cou%3Dapplications%2Cdc%3Dvdi%2Cdc%3Dvmware%2Cdc%3Dint`.

Si vous spécifiez un ID de poste de travail ou d'application, vous ne devez utiliser que des lettres minuscules, même si l'ID de poste de travail ou d'application contient des lettres majuscules dans ADSI Edit.

Note Plusieurs applications publiées ou des postes de travail distants peuvent avoir le même nom d'affichage, mais l'ID de poste de travail et d'application est unique. Pour spécifier un poste de travail distant ou une application publiée spécifique, utilisez l'ID de poste de travail ou d'application plutôt que le nom d'affichage.

query-part

Les options de configuration à utiliser, ou actions effectuées par le poste de travail distant ou l'application publiée. Les requêtes ne sont pas sensibles à la casse. Pour utiliser plusieurs requêtes, utilisez une esperluette (&) entre les requêtes. Si les requêtes sont en conflit, Horizon Client utilise la dernière requête de la liste. Utilisez la syntaxe suivante.

```
query1=value1[&query2=value2...]
```

Requêtes prises en charge

Les requêtes suivantes sont prises en charge pour ce type d'instance d'Horizon Client. Si vous créez des URI pour plusieurs types de clients, tels que des clients de poste de travail et des clients mobiles, consultez le guide d'installation et de configuration de chaque type de système client pour obtenir la liste des requêtes prises en charge.

action

Tableau 3-2. Valeurs pouvant être utilisées avec la Requête d'action

Valeur	Description
`browse`	Affiche la liste des postes de travail distants et applications publiées disponibles hébergés sur le serveur spécifié. Il ne vous est pas demandé de spécifier un poste de travail distant ou une application publiée lors de l'utilisation de cette action.
`start-session`	Ouvre l'application publiée ou le poste de travail distant spécifié(e). Si aucune requête d'action n'est fournie et que le nom du poste de travail distant ou de l'application publiée est fourni, `start-session` est l'action par défaut.
`reset`	Éteint puis redémarre le poste de travail distant ou l'application publiée spécifié(e). Les données non enregistrées sont perdues. La réinitialisation d'un poste de travail distant équivaut à appuyer sur le bouton Réinitialiser d'un ordinateur physique.

Tableau 3-2. Valeurs pouvant être utilisées avec la Requête d'action (suite)

Valeur	Description
`restart`	Éteint puis redémarre le poste de travail distant spécifié. Le redémarrage d'un poste de travail distant équivaut à la commande de redémarrage du système d'exploitation Windows. En général, le système d'exploitation invite l'utilisateur à enregistrer toutes les données non enregistrées avant de redémarrer.
`logoff`	Déconnecte l'utilisateur du système d'exploitation invité sur le poste de travail distant. Si vous spécifiez une application publiée, l'action est ignorée ou l'utilisateur final voit le message d'avertissement « Action d'URI non valide ».

args

Spécifie les arguments de ligne de commande à ajouter au démarrage de l'application publiée. Utilisez la syntaxe `args=`*value*, où *value* est une chaîne. Utilisez l'encodage avec pourcentage pour les caractères suivants :

- Pour un deux-points (:), utilisez **`%3A`**
- Pour une barre oblique inversée (\), utilisez **`%5C`**
- Pour un espace ( ), utilisez **`%20`**
- Pour un guillemet double ("), utilisez **`%22`**

Par exemple, pour spécifier le nom de fichier "`My new file.txt`" pour l'application Notepad++, utilisez **`%22My%20new%20file.txt%22`**.

appProtocol

Pour les applications publiées, les valeurs valides sont **`PCOIP`** et **`BLAST`**. Par exemple, pour spécifier le protocole PCoIP, utilisez la syntaxe **`appProtocol=PCOIP`**.

connectUSBOnInsert

Connecte un périphérique USB au poste de travail distant ou à l'application publiée au premier plan lorsque vous branchez le périphérique. Cette requête est implicitement définie si vous spécifiez la requête `unattended` pour un poste de travail distant. Pour utiliser cette requête, vous devez paramétrer la requête `action` sur **`start-session`** ou ne pas utiliser de requête `action`. Les valeurs valides sont **`true`** et **`false`**. Exemple de syntaxe : **`connectUSBOnInsert=true`**.

connectUSBOnStartup

Redirige tous les périphériques USB actuellement connectés au système client vers le poste de travail distant ou l'application publiée. Cette requête est implicitement définie si vous spécifiez la requête `unattended` pour un poste de travail distant. Pour utiliser cette requête, vous devez paramétrer la requête `action` sur **`start-session`** ou ne pas utiliser de requête `action`. Les valeurs valides sont **`true`** et **`false`**. Exemple de syntaxe : **`connectUSBOnStartup=true`**.

desktopLayout

Définit la taille de la fenêtre du poste de travail distant. Pour utiliser cette requête, vous devez définir la requête `action` sur **`start-session`** ou ne pas utiliser de requête `action`.

Tableau 3-3. Valeurs valides pour la requête desktopLayout

Valeur	Description
`fullscreen`	Un moniteur affiche son contenu en plein écran. Il s'agit de la valeur par défaut.
`multimonitor`	Tous les moniteurs affichent leur contenu en plein écran.
`windowLarge`	Fenêtre de grande taille.
`windowSmall`	Fenêtre de petite taille.
*W*x*H*	Personnalisez la résolution, spécifiez la largeur et la hauteur en pixels. Exemple de syntaxe : **`desktopLayout=1280x800`**.

desktopProtocol

Pour les postes de travail distants, les valeurs valides sont **`RDP`**, **`PCOIP`** et **`BLAST`**. Par exemple, pour spécifier le protocole PCoIP, utilisez la syntaxe **`desktopProtocol=PCOIP`**.

domainName

Spécifie le nom de domaine NETBIOS associé à l'utilisateur qui se connecte au poste de travail distant ou à l'application publiée. Utilisez par exemple `monentreprise` plutôt que `monentreprise.com`.

filePath

Spécifie le chemin d'accès au fichier sur le système local que vous voulez ouvrir avec l'application publiée. Vous devez spécifier le chemin d'accès complet, y compris la lettre de lecteur. Utilisez l'encodage avec pourcentage pour les caractères suivants :

- Pour un deux-points (:), utilisez **`%3A`**
- Pour une barre oblique inversée (\), utilisez **`%5C`**
- Pour un espace ( ), utilisez **`%20`**

Par exemple, pour représenter le chemin d'accès au fichier `C:\test file.txt`, utilisez **`C%3A%5Ctest%20file.txt`**.

launchMinimized

Démarre Horizon Client en mode réduit. Horizon Client reste réduit jusqu'au redémarrage du poste de travail distant ou de l'application publiée spécifié. La syntaxe est **`launchMinimized=true`**. Vous ne pouvez pas utiliser cette requête avec la requête **unattended**.

tokenUserName

Spécifie le nom d'utilisateur RSA ou RADIUS. N'utilisez cette requête que si le nom d'utilisateur RSA ou RADIUS est différent du nom d'utilisateur Active Directory. Si vous ne spécifiez pas cette requête et que l'authentification RSA ou RADIUS est nécessaire, Horizon Client utilise le nom d'utilisateur Windows. La syntaxe se présente ainsi : **tokenUserName=*name***.

unattended

Établit une connexion serveur avec un poste de travail distant en mode kiosque. Si vous utilisez cette requête, ne spécifiez pas d'informations utilisateur si vous avez généré le nom du compte à partir de l'adresse MAC du périphérique client. Si vous avez créé des noms de comptes personnalisés dans ADAM, par exemple des noms qui commencent par « custom- », vous devez spécifier les informations du compte.

useExisting

Si cette option est définie sur **true**, il n'est possible d'exécuter qu'une seule instance d'Horizon Client. Si des utilisateurs tentent de se connecter à un deuxième serveur, ils doivent se déconnecter du premier serveur, ce qui entraîne la déconnexion des sessions d'application publiée et de poste de travail distant. Si cette option est définie sur **false**, il est possible d'exécuter plusieurs instances d'Horizon Client et les utilisateurs peuvent se connecter à plusieurs serveurs en même temps. La valeur par défaut est **true**. Exemple de syntaxe : **useExisting=false**.

unauthenticatedAccessEnabled

Si cette option est définie sur **true**, la fonctionnalité Accès non authentifié est activée par défaut. L'option **Se connecter de manière anonyme à l'aide de l'accès non authentifié** est affichée dans l'interface utilisateur et sélectionnée. Si cette option est définie sur **false**, la fonctionnalité Accès non authentifié est désactivée. L'option **Se connecter de manière anonyme à l'aide de l'accès non authentifié** est masquée et désactivée. Lorsque cette option est définie sur `""`, la fonctionnalité Accès non authentifié est désactivée et le paramètre **Se connecter de manière anonyme à l'aide de l'accès non authentifié** n'apparaît pas sur l'interface utilisateur et est désactivé. Exemple de syntaxe : **unauthenticatedAccessEnabled=true**.

unauthenticatedAccessAccount

Si la fonctionnalité Accès non authentifié est activée, définit le compte à utiliser. Si la fonctionnalité Accès non authentifié est désactivée, cette requête est ignorée. Exemple de syntaxe utilisant le compte d'utilisateur **anonymous1** : **unauthenticatedAccessAccount=anonymous1**.

Exemples d'URI de vmware-view

Vous pouvez utiliser le schéma d'URI `vmware-view` pour créer des liens hypertextes ou des boutons et inclure ces liens dans un e-mail ou sur une page Web. Par exemple, un utilisateur

final peut cliquer un lien d'URI pour démarrer un poste de travail distant avec les options de démarrage que vous spécifiez.

Exemples de syntaxe URI

Chaque exemple d'URI est suivi d'une description de ce que l'utilisateur final voit après avoir cliqué sur le lien URI.

1 `vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session`

Horizon Client démarre et se connecte au serveur `view.mycompany.com`. La boîte de dialogue de connexion invite l'utilisateur à fournir un nom d'utilisateur, un nom de domaine et un mot de passe. Après l'ouverture de session, le client se connecte au poste de travail distant dont le nom d'affichage est `Poste de travail principal`, et l'utilisateur est connecté au système d'exploitation client.

Note Dans cet exemple, le protocole d'affichage et la taille de fenêtre par défaut sont utilisés. Le protocole d'affichage par défaut est PCoIP et la taille de fenêtre par défaut est le mode plein écran.

2 `vmware-view://view.mycompany.com/cn%3Dwin7-32%2Cou%3Dapplications%2Cdc%3Dvdi%2Cdc%3Dvmware%2Cdc%3Dint`

Horizon Client démarre et se connecte au serveur `view.mycompany.com`. La boîte de dialogue de connexion invite l'utilisateur à fournir un nom d'utilisateur, un nom de domaine et un mot de passe. Après une ouverture de session réussie, le client se connecte au poste de travail distant disposant de l'ID de poste de travail `CN=win7-32,OU=Applications,DC=vdi,DC=vmware,DC=int` (encoded value `cn%3Dwin7-32%2Cou%3Dapplications%2Cdc%3Dvdi%2Cdc%3Dvmware%2Cdc%3Dint`).

3 `vmware-view://view.mycompany.com:7555/Primary%20Desktop`

Cet URI a le même effet que dans l'exemple précédent, sauf qu'il utilise le port non défini par défaut 7555 pour l'instance du Serveur de connexion. (Le port par défaut est 443.) Comme un identifiant de poste de travail distant est fourni, le poste de travail distant s'ouvre même si l'action `start-session` n'est pas incluse dans l'URI.

4 `vmware-view://fred@view.mycompany.com/Finance%20Desktop?desktopProtocol=PCOIP`

Horizon Client démarre et se connecte au serveur `view.mycompany.com`. Dans la boîte de dialogue de connexion, la zone de texte **Nom d'utilisateur** contient le nom `fred`. L'utilisateur doit fournir le nom de domaine et le mot de passe. Après l'ouverture de session, le client se connecte au poste de travail distant dont le nom d'affichage est `Poste de travail Finance`, et l'utilisateur est connecté au système d'exploitation client. La connexion utilise le protocole d'affichage PCoIP.

5 `vmware-view://view.mycompany.com/Calculator?action=start-session&appProtocol=BLAST`

Horizon Client démarre et se connecte au serveur `view.mycompany.com`. Dans la boîte de dialogue de connexion, l'utilisateur doit fournir le nom d'utilisateur, le nom de domaine et le mot de passe. Après la connexion, le client se connecte à l'application publiée dont le nom d'affichage est `Calculatrice`. La connexion utilise le protocole d'affichage VMware Blast.

6
```
vmware-view://fred@view.mycompany.com/Finance%20Desktop?domainName=mycompany
```

Horizon Client démarre et se connecte au serveur `view.mycompany.com`. Dans la boîte de dialogue de connexion, la zone de texte **Nom d'utilisateur** contient le nom `fred` et la zone de texte **Domaine** contient `mycompany`. L'utilisateur doit fournir uniquement un mot de passe. Après l'ouverture de session, le client se connecte au poste de travail distant dont le nom d'affichage est `Poste de travail Finance`, et l'utilisateur est connecté au système d'exploitation client.

7
```
vmware-view://view.mycompany.com/
```

Horizon Client démarre et l'utilisateur est dirigé vers l'invite d'ouverture de session pour se connecter au serveur `view.mycompany.com`.

8
```
vmware-view://view.mycompany.com/Primary%20Desktop?action=reset
```

Horizon Client démarre et se connecte au serveur `view.mycompany.com`. La boîte de dialogue de connexion invite l'utilisateur à fournir un nom d'utilisateur, un nom de domaine et un mot de passe. Après l'ouverture de session, Horizon Client affiche une boîte de dialogue qui invite l'utilisateur à confirmer l'opération de réinitialisation du `Poste de travail principal`.

Note Cette action est disponible uniquement si un administrateur Horizon a activé la fonctionnalité de réinitialisation de poste de travail principal.

9
```
vmware-view://view.mycompany.com/Primary%20Desktop?action=restart
```

Horizon Client démarre et se connecte au serveur `view.mycompany.com`. La boîte de dialogue de connexion invite l'utilisateur à fournir un nom d'utilisateur, un nom de domaine et un mot de passe. Après l'ouverture de session, Horizon Client affiche une boîte de dialogue qui invite l'utilisateur à confirmer l'opération de redémarrage du `Poste de travail principal`.

Note Cette action est disponible uniquement si un administrateur Horizon a activé la fonctionnalité de redémarrage de poste de travail distant.

10
```
vmware-view://view.mycompany.com/Primary%20Desktop?action=start-
session&connectUSBOnStartup=true
```

Cet URI a le même effet que le premier exemple, et tous les périphériques USB connectés au système client sont redirigés vers le poste de travail distant.

11
```
vmware-view://
```

Si Horizon Client n'est pas en cours d'exécution, il démarre. Si Horizon Client est déjà en cours d'exécution, il passe au premier plan.

12
```
vmware-view://10.10.10.10/My%20Notepad++?args=%22My%20new%20file.txt%22
```

Démarre My Notepad++ sur le serveur 10.10.10.10 et transmet l'argument `My new file.txt` dans la commande de démarrage d'application publiée. Les espaces et les guillemets utilisent l'échappement de pourcentage. Le nom de fichier est entre guillemets, car il contient des espaces.

Vous pouvez également taper cette commande dans l'invite de ligne de commande Windows en utilisant la syntaxe suivante :

```
vmware-view.exe --serverURL 10.10.10.10 --appName "My Notepad++" --args "\"my new.txt\""
```

Dans cet exemple, les guillemets sont échappés avec les caractères \".

13
```
vmware-view://10.10.10.10/Notepad++%2012?args=a.txt%20b.txt
```

Démarre Notepad++ 12 sur le serveur 10.10.10.10 et transmet l'argument `a.text b.txt` dans la commande démarrage d'application publiée. Comme l'argument n'est pas entre guillemets, un espace sépare les noms de fichier et les deux fichiers sont ouverts séparément dans Notepad++.

Note Les applications publiées peuvent utiliser les arguments de ligne de commande différemment. Par exemple, si vous transmettez l'argument `a.txt b.txt` à WordPad, WordPad n'ouvre qu'un seul fichier, `a.txt`.

14
```
vmware-view://view.mycompany.com/Notepad?
unauthenticatedAccessEnabled=true&unauthenticatedAccessAccount=anonymous1
```

Horizon Client démarre et se connecte au serveur `view.mycompany.com` en utilisant le compte d'utilisateur **`anonymous1`**. L'application Notepad démarre sans inviter l'utilisateur à fournir ses informations d'identification.

Exemples de code HTML

Vous pouvez utiliser des URI pour faire des liens hypertextes et des boutons à inclure dans des e-mails ou sur des pages Web. Les exemples suivants montrent comment utiliser l'URI du premier exemple d'URI pour coder un lien hypertexte intitulé **Test Link** et un bouton intitulé **TestButton**.

```
<html>
<body>

<a href="vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session">Test Link</
a><br>
```

```
<form><input type="button" value="TestButton" onClick="window.location.href=
'vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session'"></form> <br>

</body>
</html>
```

Définition du mode de vérification des certificats dans Horizon Client

La vérification des certificats du serveur se produit pour les connexions entre Horizon Client et un serveur. Un certificat est une forme numérique d'identification, semblable à un passeport ou à un permis de conduire.

La vérification des certificats du serveur inclut les vérifications suivantes :

- Le certificat a-t-il été révoqué ?
- Le certificat a-t-il un autre but que de vérifier l'identité de l'expéditeur et de chiffrer les communications du serveur ? Autrement dit, s'agit-il du bon type de certificat ?
- Le certificat a-t-il expiré, ou est-il valide uniquement dans le futur ? Autrement dit, le certificat est-il valide en fonction de l'horloge de l'ordinateur ?
- Le nom commun sur le certificat correspond-il au nom d'hôte du serveur qui l'envoie ? Une incompatibilité peut se produire si l'équilibrage de charge redirige Horizon Client vers un serveur disposant d'un certificat qui ne correspond pas au nom d'hôte entré dans Horizon Client. Une incompatibilité peut également se produire si vous entrez une adresse IP plutôt qu'un nom d'hôte dans le client.
- Le certificat est-il signé par une autorité de certification inconnue ou non approuvée ? Les certificats auto-signés sont un type d'autorité de certification non approuvée. Pour que cette vérification aboutisse, la chaîne d'approbation du certificat doit être associée à une racine dans le magasin de certificats local.

Pour plus d'informations sur la distribution d'un certificat racine auto-signé à tous les systèmes clients Windows dans un domaine, consultez « Ajouter le certificat racine aux autorités de certification racine approuvées » dans le document *Installation d'Horizon*.

Pour définir le mode de vérification des certificats, démarrez Horizon Client et sélectionnez **Configurer SSL** dans le menu **Options** sur la barre de menus Horizon Client. Vous pouvez sélectionner l'une des options suivantes.

- **Ne jamais se connecter à des serveurs non autorisés**. Ce paramètre signifie que vous ne pouvez pas vous connecter au serveur si une des vérifications de certificat échoue. Un message d'erreur répertorie les vérifications qui ont échoué.

- **Signaler avant de se connecter à des serveurs non autorisés**. Ce paramètre signifie que vous pouvez cliquer sur **Continuer** pour ignorer l'avertissement si une vérification de certificat échoue, car le serveur utilise un certificat auto-signé. Pour les certificats auto-signés, le nom du certificat ne doit pas nécessairement correspondre au nom de serveur que vous avez entré dans Horizon Client. Vous pouvez également recevoir un avertissement si le certificat a expiré.
- **Ne pas vérifier les certificats d'identité des serveurs**. Ce paramètre signifie qu'aucune vérification des certificats n'a lieu.

Si un administrateur installe ultérieurement un certificat de sécurité à partir d'une autorité de certification de confiance et que toutes les vérifications de certificat réussissent lorsque vous vous connectez, cette connexion approuvée est enregistrée pour ce serveur spécifique. À l'avenir, si ce serveur présente de nouveau un certificat auto-signé, la connexion échoue. Après qu'un serveur particulier présente un certificat entièrement vérifiable, il doit toujours faire ainsi.

Important Si vous avez utilisé précédemment une stratégie de groupe pour configurer les systèmes clients de votre société pour utiliser un chiffrement spécifique, par exemple en configurant les paramètres de stratégie de groupe SSL Cipher Suite Order, vous devez maintenant utiliser un paramètre de sécurité de stratégie de groupe Horizon Client. Reportez-vous à la section Paramètres de sécurité des objets de stratégie de groupe (GPO) des clients. Vous pouvez également utiliser le paramètre de registre `SSLCipherList` sur le système client. Reportez-vous à la section Utilisation du Registre Windows pour configurer Horizon Client.

Vous pouvez configurer le mode de vérification des certificats par défaut et empêcher les utilisateurs finaux de le modifier dans Horizon Client. Pour plus d'informations, reportez-vous à la section Configuration du mode de vérification des certificats pour les utilisateurs finaux.

Utilisation d'un serveur proxy SSL

Si vous utilisez un serveur proxy SSL pour inspecter le trafic envoyé depuis l'environnement client vers Internet, activez le paramètre **Autoriser la connexion via un proxy SSL**. Ce paramètre permet la vérification des certificats pour les connexions secondaires via un serveur proxy SSL et s'applique aux connexions Blast Secure Gateway et de tunnel sécurisé. Si vous utilisez un serveur proxy SSL et que vous activez la vérification des certificats, mais que vous n'activez pas le paramètre **Autoriser la connexion via un proxy SSL**, les connexions échouent en raison d'empreintes numériques incompatibles. Le paramètre **Autoriser la connexion via un proxy SSL** n'est pas disponible si vous activez l'option **Ne pas vérifier les certificats d'identité des serveurs**. Lorsque l'option **Ne pas vérifier les certificats d'identité des serveurs** est activée, Horizon Client ne vérifie pas le certificat ou l'empreinte numérique et un proxy SSL est toujours autorisé.

Vous pouvez utiliser le paramètre de stratégie de groupe **Configure le comportement de vérification des certificats de proxy SSL d'Horizon Client** pour configurer l'autorisation de vérification des certificats pour les connexions secondaires via un serveur proxy SSL. Pour plus d'informations, consultez le document Paramètres de sécurité des objets de stratégie de groupe (GPO) des clients.

Pour autoriser les connexions VMware Blast via un serveur proxy, voir Configurer des options VMware Blast.

Configuration du mode de vérification des certificats pour les utilisateurs finaux

Vous pouvez configurer le mode de vérification des certificats pour les utilisateurs finaux. Par exemple, vous pouvez spécifier qu'une vérification complète doit toujours être effectuée. La vérification des certificats est efectuée pour les connexions TLS entre un serveur et Horizon Client.

Vous pouvez configurer une des stratégies de vérification des certificats suivantes pour les utilisateurs finaux.

- Les utilisateurs finaux sont autorisés à sélectionner le mode de vérification des certificats dans Horizon Client.
- (Pas de vérification) Aucune vérification de certificat n'est effectuée.
- (Avertir) Si le serveur présente un certificat auto-signé, les utilisateurs sont avertis. Les utilisateurs peuvent choisir d'autoriser ou non ce type de connexion.
- (Sécurité complète) Une vérification complète est effectuée et les connexions qui ne passent pas de vérification complète sont rejetées.

Si vous utilisez un serveur proxy SSL pour inspecter le trafic envoyé depuis l'environnement client vers Internet, vous pouvez configurer la vérification des certificats pour les connexions secondaires via le serveur proxy SSL. Cette fonctionnalité s'applique aux connexions Blast Secure Gateway et aux connexions tunnel. Vous pouvez également autoriser l'utilisation du serveur proxy pour les connexions VMware Blast.

Pour plus d'informations sur les types de vérifications des certificats pouvant être effectués, reportez-vous à la section Définition du mode de vérification des certificats dans Horizon Client.

Vous pouvez utiliser les paramètres de stratégie de groupe d'Horizon Client pour définir le mode de vérification des certificats, autoriser l'utilisation du proxy SSL, limiter l'utilisation de certains algorithmes et protocoles de chiffrement avant d'établir une connexion TLS chiffrée et activer l'utilisation de proxy pour les connexions VMware Blast. Pour plus d'informations, consultez Paramètres de sécurité des objets de stratégie de groupe (GPO) des clients et Paramètres généraux des objets de stratégie de groupe (GPO) de clients.

Si vous ne souhaitez pas configurer le paramètre de vérification des certificats en tant que stratégie de groupe, vous pouvez activer la vérification des certificats en ajoutant le nom de valeur `CertCheckMode` à l'une des clés de registre suivantes sur l'ordinateur client :

- Pour Windows 32 bits : `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security`
- Pour Windows 64 bits : `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security`

Utilisez les valeurs suivantes dans la clé de registre :

- **0** implémente `Do not verify server identity certificates.`
- **1** implémente `Warn before connecting to untrusted servers.`
- **2** implémente `Never connect to untrusted servers.`

Si vous configurez le paramètre de stratégie de groupe et le paramètre `CertCheckMode` dans la clé de registre, le paramètre de stratégie de groupe est prioritaire sur la valeur de la clé de registre.

Configuration des options TLS avancées

Vous pouvez sélectionner les protocoles de sécurité et les algorithmes de chiffrement qui sont utilisés pour chiffrer les communications entre Horizon Client et des serveurs et entre Horizon Client et l'agent dans un poste de travail distant.

Ces options de sécurité sont également utilisées pour chiffrer le canal USB.

Avec le paramètre par défaut, les suites de chiffrement utilisent la spécification AES 128 ou 256 bits, suppriment les algorithmes DH anonymes, puis trient la liste de chiffrements actuelle par longueur de clé d'algorithme de chiffrement.

Par défaut, TLS v1.1 et TLS v1.2 sont activés. SSL v2.0, SSL v3.0 et TLS v1.0 ne sont pas pris en charge.

Si vous configurez un protocole de sécurité pour Horizon Client qui n'est pas activé sur le serveur auquel le client se connecte, une erreur TLS se produit et la connexion échoue.

Important Au moins un des protocoles que vous activez dans Horizon Client doit être également activé sur le poste de travail distant pour que les périphériques USB puissent être redirigés vers le poste de travail distant.

Sur le système client, vous pouvez utiliser un paramètre de stratégie de groupe ou un paramètre de Registre Windows pour modifier les chiffrements et protocoles par défaut. Pour plus d'informations sur l'utilisation d'un paramètre de stratégie de groupe, reportez-vous au paramètre **Configurer les protocoles SSL et les algorithmes de chiffrement** dans Paramètres de sécurité des objets de stratégie de groupe (GPO) des clients. Pour plus d'informations sur l'utilisation du paramètre SSLCipherList dans le Registre Windows, reportez-vous à Utilisation du Registre Windows pour configurer Horizon Client.

Personnalisation des menus d'Horizon Client

Vous pouvez utiliser des stratégies de groupe d'Horizon Client afin de masquer certains éléments dans certains menus de l'interface utilisateur d'Horizon Client.

Pour obtenir des informations générales sur l'utilisation de stratégies de groupe d'Horizon Client, reportez-vous à la section Utilisation de paramètres de stratégie de groupe pour configurer Horizon Client.

Pour obtenir des informations détaillées sur l'utilisation des stratégies de groupe qui contrôlent les menus d'Horizon Client, reportez-vous aux descriptions des paramètres de stratégie de groupe **Masquer des éléments dans le menu contextuel de l'application**, **Masquer des éléments dans le menu contextuel du poste de travail**, **Masquer des éléments dans la barre d'outils du poste de travail**, **Masquer des éléments dans le menu de la barre d'état système** et **Masquer des éléments dans le menu de la barre d'outils du client** dans la section Paramètres généraux des objets de stratégie de groupe (GPO) de clients.

Personnalisation des messages d'erreur d'Horizon Client

Vous pouvez utiliser le paramètre de stratégie de groupe Horizon ClientPied de page de l'écran d'erreur personnalisé d' pour ajouter du texte d'aide personnalisé au bas de tous les messages d'erreur qui s'affichent dans l'interface utilisateur d'Horizon Client. Par exemple, votre texte d'aide peut indiquer aux utilisateurs comment contacter le support technique de votre entreprise.

Vous devez créer un fichier de texte brut (`.txt`) sur le système client local pour qu'il contienne le texte d'aide. Le fichier texte peut contenir jusqu'à 2 048 caractères, y compris des caractères de contrôle. Les encodages ANSI et Unicode sont tous deux pris en charge. Vous spécifiez le chemin d'accès complet à ce fichier texte lorsque vous configurez le paramètre de stratégie de groupe **Pied de page de l'écran d'erreur personnalisé**.

Pour obtenir des informations générales sur l'utilisation de stratégies de groupe d'Horizon Client, reportez-vous à la section Utilisation de paramètres de stratégie de groupe pour configurer Horizon Client.

Pour obtenir des informations détaillées sur l'utilisation du paramètre de stratégie de groupe **Pied de page de l'écran d'erreur personnalisé**, reportez-vous à la section Paramètres généraux des objets de stratégie de groupe (GPO) de clients.

Configuration de la gestion des événements du curseur

Pour optimiser la gestion des événements du curseur, configurez les paramètres dans le fichier `C:\ProgramData\VMware\VMware Horizon View\config.ini` sur le système client Windows.

Note Pour utiliser la gestion des événements du curseur, vous devez installer Horizon Agent 2006 ou version ultérieure sur le poste de travail distant.

Paramètre	Description
`RemoteDisplay.allowCursorWarping`	Active ou désactive la fonctionnalité de distorsion du curseur. Lorsque cette fonctionnalité est activée et que la souris est en mode absolu, l'agent distant détecte les mouvements soudains du curseur et les répercute sur le client en déplaçant le curseur local. Lorsque cette fonctionnalité est désactivée, le client ignore les mouvements soudains du curseur dans l'agent distant. Les valeurs valides sont TRUE ou FALSE. La valeur par défaut est TRUE.
`RemoteDisplay.allowCursorEventsOnLowLatencyChannel`	Détermine si le canal à faible latence est utilisé pour les mises à jour du curseur. Les valeurs valides sont TRUE ou FALSE. La valeur par défaut est TRUE.

Pour configurer la latence maximale autorisée lors de la fusion des mouvements de la souris, définissez le paramètre de stratégie de groupe **Configurer la latence maximale pour la fusion de la souris**. Pour plus d'informations, reportez-vous à la section Paramètres généraux des objets de stratégie de groupe (GPO) de clients.

Vous pouvez également configurer la gestion des événements du curseur sur la machine agent. Par exemple, vous pouvez utiliser le paramètre de stratégie de groupe **Distorsion du curseur** côté agent pour configurer la distorsion du curseur. Vous pouvez également modifier les paramètres de Registre Windows sur la machine agent pour activer ou désactiver la fusion des événements de déplacement de la souris et du canal à faible latence. Pour que la fonctionnalité soit activée, les paramètres du client et de l'agent doivent correspondre. Pour plus d'informations sur les paramètres côté agent, consultez le document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Utilisation de paramètres de stratégie de groupe pour configurer Horizon Client

Horizon Client inclut un modèle de fichier d'administration ADMX de stratégie de groupe que vous pouvez utiliser pour configurer les fonctionnalités et le comportement d'Horizon Client. Vous pouvez optimiser et sécuriser les connexions aux applications publiées et aux postes de travail distants en ajoutant les paramètres de stratégie du modèle de fichier ADMX à un nouveau GPO ou à un GPO existant dans Active Directory.

Le fichier de modèle contient des stratégies de groupe Configuration d'ordinateur et Configuration d'utilisateur.

- Les stratégies Configuration d'ordinateur définissent des stratégies qui s'appliquent à Horizon Client, sans tenir compte de la personne qui exécute le client sur l'hôte.
- Les stratégies de configuration d'utilisateur définissent des stratégies Horizon Client qui s'appliquent à tous les utilisateurs qui exécutent Horizon Client, ainsi qu'aux paramètres de connexion RDP. Les stratégies Configuration d'utilisateur remplacent les stratégies Configuration d'ordinateur équivalentes.

Horizon Client applique les stratégies lorsque les applications publiées et les postes de travail démarrent et lorsque les utilisateurs se connectent.

Le fichier de modèle ADMX de configuration d'Horizon Client (`vdm_client.admx`) et tous les fichiers de modèle ADMX qui fournissent les paramètres de stratégie de groupe sont disponibles dans le dossier `VMware-Horizon-Extras-Bundle-YYMM-x.x.x-yyyyyyy.zip`, où *YYMM* est le numéro de version marketing, *x.x.x* est le numéro de version interne et *yyyyyyy* est le numéro de build. Vous pouvez télécharger ce fichier ZIP depuis le site de téléchargement VMware à l'adresse https://my.vmware.com/web/vmware/downloads. Vous devez copier le fichier sur votre serveur Active Directory et utiliser l'éditeur de gestion des stratégies de groupes pour ajouter les modèles d'administration. Pour obtenir des instructions, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Paramètres de définition de scripts des objets de stratégie de groupe (GPO) des clients

Vous pouvez définir des stratégies de groupe pour un grand nombre des paramètres que vous pouvez configurer lorsque vous exécutez Horizon Client depuis la ligne de commande, notamment la taille de la fenêtre de poste de travail distant, le nom d'utilisateur de connexion et le nom de domaine de connexion.

Le tableau suivant décrit les paramètres de définition de script du fichier de modèle ADMX de configuration de VMware Horizon Client. Ce modèle de fichier fournit une version de configuration d'ordinateur et de configuration d'utilisateur de chaque paramètre de définition de script. Le paramètre de Configuration d'utilisateur remplace le paramètre de Configuration d'ordinateur équivalent. Les paramètres se trouvent dans le dossier **Configuration de VMware Horizon Client > Définitions de script** de l'éditeur de gestion de stratégie de groupe.

Tableau 3-4. Modèle de configuration de VMware Horizon Client : définitions de scripts

Paramètre	Description
`Automatically connect if only one launch item is entitled`	Si un utilisateur est autorisé à n'utiliser qu'un seul poste de travail distant, il connecte l'utilisateur à ce poste de travail distant. Ce paramètre évite à l'utilisateur d'avoir à sélectionner le poste de travail distant dans une liste n'en contenant qu'un seul.
`Connect all USB devices to the desktop or remote application on launch`	Détermine si tous les périphériques USB disponibles sur le système client sont connectés au poste de travail distant ou à l'application publiée lorsque le poste de travail distant ou l'application publiée démarre.
`Connect USB devices to the desktop or remote application when they are plugged in`	Détermine si les périphériques USB sont connectés au poste de travail distant ou à l'application publiée lorsqu'ils sont branchés sur le système client.

Tableau 3-4. Modèle de configuration de VMware Horizon Client : définitions de scripts (suite)

Paramètre	Description
`DesktopLayout`	Spécifie la disposition de la fenêtre Horizon Client que les utilisateurs voient lorsqu'ils se connectent à un poste de travail distant. Les différentes dispositions sont les suivantes : ■ `Full Screen` ■ `Multimonitor` ■ `Window - Large` ■ `Window - Small` Ce paramètre n'est disponible que lorsque le paramètre `DesktopName to select setting` est également défini.
`DesktopName to select`	Spécifie le poste de travail par défaut utilisé par Horizon Client lors de la connexion.
`Disable 3rd-party Terminal Services plugins`	Détermine si Horizon Client doit vérifier les plug-ins Services Terminal Server installés en tant que plug-ins RDP normaux. Si vous ne configurez pas ce paramètre,Horizon Client vérifie les plug-ins tiers par défaut. Ce paramètre n'affecte pas les plug-ins spécifiques d'Horizon, comme la redirection USB.
`Locked Guest Size`	Si l'affichage est utilisé sur un seul moniteur, spécifie la résolution d'écran du poste de travail distant. Ce paramètre ne fonctionne pas si vous avez configuré l'affichage du poste de travail distant sur **Tous les moniteurs**. Après avoir activé ce paramètre, la fonctionnalité d'ajustement automatique du poste de travail distant est désactivée et l'option **Autoriser la mise à l'échelle de l'affichage** est masquée dans l'interface utilisateur d'Horizon Client.
`Logon DomainName`	Spécifie le domaine NetBIOS utilisé par Horizon Client lors de la connexion.
`Logon Password`	Spécifie le mot de passe utilisé par Horizon Client lors de la connexion. Active Directory stocke ce mot de passe en texte brut. Pour améliorer la sécurité, ne spécifiez pas ce paramètre. Les utilisateurs peuvent entrer le mot de passe de façon interactive.
`Logon UserName`	Spécifie le mot de passe utilisé par Horizon Client lors de la connexion. Active Directory stocke ce mot de passe en texte brut.
`Server URL`	Spécifie l'URL utilisée par Horizon Client lors de la connexion. Par exemple, `https://view1.example.com`.
`Suppress error messages (when fully scripted only)`	Détermine si les messages d'erreur d'Horizon Client doivent être masqués lors de la connexion. Ce paramètre ne s'applique que lorsque le processus d'ouverture de session est entièrement scripté, par exemple, lorsque toutes les informations d'ouverture de session requises sont préremplies par la stratégie de groupe. Si la connexion échoue en raison d'informations de connexion incorrectes, les utilisateurs ne sont pas avertis et le processus Horizon Client est interrompu.

Tableau 3-4. Modèle de configuration de VMware Horizon Client : définitions de scripts (suite)

Paramètre	Description
`Disconnected application session resumption behavior`	Détermine comment les applications publiées en cours d'exécution se comportent lorsque des utilisateurs se reconnectent à un serveur. Les choix sont les suivants : ■ Demander la reconnexion pour ouvrir des applications ■ Se reconnecter automatiquement pour ouvrir des applications ■ Ne pas demander et ne pas se reconnecter automatiquement Lorsque ce paramètre est activé, les utilisateurs finaux ne peuvent pas configurer le comportement de reconnexion aux applications publiées dans Horizon Client. Lorsque ce paramètre est désactivé, les utilisateurs finaux peuvent configurer le comportement de reconnexion aux applications publiées dans Horizon Client. Ce paramètre est désactivé par défaut.
`Enable Unauthenticated Access to the server`	Détermine si des utilisateurs doivent entrer des informations d'identification pour accéder à leurs applications publiées lorsqu'ils utilisent Horizon Client. Lorsque ce paramètre est activé, le paramètre **Se connecter de manière anonyme à l'aide de l'accès non authentifié** dans Horizon Client est affiché, désactivé et sélectionné. Le client peut revenir à une autre méthode d'authentification si l'accès non authentifié n'est pas disponible. Lorsque ce paramètre est désactivé, les utilisateurs doivent toujours entrer leurs informations d'identification pour se connecter et accéder à leurs applications publiées. Le paramètre **Se connecter de manière anonyme à l'aide de l'accès non authentifié** dans Horizon Client est masqué et désélectionné. Les utilisateurs peuvent activer l'accès non authentifié dans Horizon Client par défaut. Le paramètre **Se connecter de manière anonyme à l'aide de l'accès non authentifié** est affiché, activé et désélectionné.
`Account to use for Unauthenticated Access`	Spécifie le compte d'utilisateur Accès non authentifié qu'Horizon Client utilise pour se connecter de manière anonyme au serveur si le paramètre de stratégie de groupe `Enable Unauthenticated Access to the server` est activé ou si un utilisateur active l'accès non authentifié en sélectionnant **Se connecter de manière anonyme à l'aide de l'accès non authentifié** dans Horizon Client. Si l'accès non authentifié n'est pas utilisé pour une connexion spécifique à un serveur, ce paramètre est ignoré. Les utilisateurs peuvent sélectionner un compte par défaut.
`Use existing client instance when connect to same server`	Détermine si une connexion est ajoutée à l'instance existante d'Horizon Client avec laquelle l'utilisateur est déjà connecté au même serveur. Ce paramètre est désactivé par défaut lorsqu'il n'est pas configuré.

Paramètres de sécurité des objets de stratégie de groupe (GPO) des clients

Les paramètres de sécurité incluent les stratégies de groupe pour les certificats, les informations d'identification et la fonctionnalité d'authentification unique.

Le tableau suivant décrit les paramètres de sécurité figurant dans le fichier de modèle ADMX de configuration d'Horizon Client. Ce tableau montre si les paramètres incluent à la fois les paramètres Configuration ordinateur et Configuration utilisateur, ou uniquement les paramètres Configuration ordinateur. Pour les paramètres de sécurité qui incluent les deux types de paramètres, le paramètre User Configuration (Configuration utilisateur) remplace le paramètre Computer Configuration (Configuration ordinateur) équivalent. Ces paramètres se trouvent dans le dossier **Configuration de VMware Horizon Client > Paramètres de sécurité** de l'éditeur de gestion de stratégie de groupe.

Tableau 3-5. Modèle de configuration d'Horizon Client : paramètres de sécurité

Paramètre	Ordinateur	Utilisateur	Description
`Allow command line credentials`	X		Détermine si les informations d'identification d'utilisateur peuvent être fournies avec des options de ligne de commande d'Horizon Client. Si ce paramètre est désactivé, les options `smartCardPIN` et `password` ne sont pas disponibles lorsque les utilisateurs exécutent Horizon Client à partir de la ligne de commande. Ce paramètre est activé par défaut. La valeur de Registre Windows équivalente est `AllowCmdLineCredentials`.
`Configures the SSL Proxy certificate checking behavior of the Horizon Client`	X		Détermine s'il convient d'autoriser la vérification des certificats pour les connexions secondaires via un serveur proxy SSL pour les connexions Blast Secure Gateway et de tunnel sécurisé. Lorsque ce paramètre n'est pas configuré (par défaut), les utilisateurs peuvent modifier manuellement le paramètre de proxy SSL dans Horizon Client. Reportez-vous à Définition du mode de vérification des certificats dans Horizon Client. Par défaut, Horizon Client bloque les connexions proxy SSL des connexions Blast Secure Gateway et de tunnel sécurisé.

Tableau 3-5. Modèle de configuration d'Horizon Client : paramètres de sécurité (suite)

Paramètre	Ordinateur	Utilisateur	Description
`Servers Trusted For Delegation`	X		Spécifie les instances du Serveur de connexion qui acceptent l'identité de l'utilisateur et les informations d'identification qui sont transmises lorsqu'un utilisateur sélectionne **Se connecter en tant qu'utilisateur actuel** dans le menu **Options** de la barre de menus Horizon Client. Si vous ne spécifiez pas d'instances du Serveur de connexion, toutes les instances du Serveur de connexion acceptent ces informations, sauf si le paramètre d'authentification **Autoriser l'ouverture de session en tant qu'utilisateur actuel** est désactivé pour l'instance du Serveur de connexion dans Horizon Console. Pour ajouter une instance de Serveur de connexion, utilisez l'un des formats suivants : ■ `domain\system$` ■ `system$@domain.com` ■ Nom principal de service (SPN) du service Serveur de connexion. La valeur de Registre Windows équivalente est `BrokersTrustedForDelegation`.

Tableau 3-5. Modèle de configuration d'Horizon Client : paramètres de sécurité (suite)

Paramètre	Ordinateur	Utilisateur	Description
`Certificate verification mode`	X		Configure le niveau de vérification des certificats exécutée par Horizon Client. Vous pouvez sélectionner l'un de ces modes : ■ `No Security`. Aucune vérification des certificats n'est exécutée. ■ `Warn But Allow`. Si une vérification de certificat échoue car le serveur utilise un certificat auto-signé, les utilisateurs voient un avertissement, qu'ils peuvent ignorer. Pour les certificats autosignés, le nom du certificat ne doit pas nécessairement correspondre au nom du serveur que les utilisateurs ont entré dans Horizon Client. Si une autre condition d'erreur de certificat se produit, Horizon Client affiche une erreur et empêche les utilisateurs de se connecter au serveur. `Warn But Allow` est la valeur par défaut. ■ `Full Security`. Si une erreur de type de certificat se produit, les utilisateurs ne peuvent pas se connecter au serveur. Horizon Client affiche les erreurs de certificat à l'utilisateur. Lorsque ce paramètre est configuré, les utilisateurs peuvent afficher le mode de vérification de certificat sélectionné dans Horizon Client, mais ils ne peuvent pas configurer le paramètre. La boîte de dialogue du mode de vérification des certificats informe les utilisateurs qu'un administrateur a verrouillé le paramètre. Lorsque ce paramètre est désactivé, les utilisateurs d'Horizon Client peuvent sélectionner un mode de vérification des certificats. Ce paramètre est désactivé par défaut. Pour autoriser un serveur à sélectionner les certificats fournis par Horizon Client, le client doit établir des connexions HTTPS avec l'hôte du Serveur de connexion ou du serveur de sécurité. La vérification des certificats n'est pas prise en charge si vous déchargez TLS vers un serveur intermédiaire qui établit des connexions HTTP avec l'hôte du Serveur de connexion ou du serveur de sécurité. Si vous ne souhaitez pas configurer ce paramètre en tant que stratégie de groupe, vous pouvez également activer la vérification de certificat en ajoutant le nom de valeur `CertCheckMode` à l'une des clés de registre suivantes sur l'ordinateur client : ■ Pour Windows 32 bits : `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security` ■ Pour Windows 64 bits : `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security`

Tableau 3-5. Modèle de configuration d'Horizon Client : paramètres de sécurité (suite)

Paramètre	Ordinateur	Utilisateur	Description
			Utilisez les valeurs suivantes dans la clé de registre : ■ **0** implémente `No Security`. ■ **1** implémente `Warn But Allow`. ■ **2** implémente `Full Security`. Si vous configurez le paramètre de stratégie de groupe et le paramètre `CertCheckMode` dans la clé de Registre Windows, le paramètre de stratégie de groupe est prioritaire sur la valeur de la clé de registre. **Note** Dans une future version d'Horizon Client, l'utilisation du registre Windows pour configurer ce paramètre ne peut pas être prise en charge et le paramètre de stratégie de groupe doit être utilisé.
`Default value of the 'Log in as current user' checkbox`	X	X	Spécifie la valeur par défaut de **Se connecter en tant qu'utilisateur actuel** dans le menu **Options** de la barre de menus Horizon Client. Ce paramètre remplace la valeur par défaut spécifiée au cours de l'installation d'Horizon Client. Si un utilisateur exécute Horizon Client à partir de la ligne de commande et spécifie l'option `logInAsCurrentUser`, cette valeur remplace ce paramètre. Lorsque l'option **Se connecter en tant qu'utilisateur actuel** est sélectionnée dans le menu **Options**, l'identité et les informations d'identification que l'utilisateur a fournies lors de la connexion au système client sont transmises à l'instance du Serveur de connexion, puis à l'application publiée ou au poste de travail distant. Lorsque l'option **Se connecter en tant qu'utilisateur actuel** est désélectionnée, les utilisateurs doivent fournir leur identité et leurs informations d'identification plusieurs fois avant de pouvoir accéder à une application publiée ou un poste de travail distant. Ce paramètre est désactivé par défaut. La valeur de Registre Windows équivalente est `LogInAsCurrentUser`.

Tableau 3-5. Modèle de configuration d'Horizon Client : paramètres de sécurité (suite)

Paramètre	Ordinateur	Utilisateur	Description
`Display option to Log in as current user`	X	X	Détermine si **Se connecter en tant qu'utilisateur actuel** est visible dans le menu **Options** de la barre de menus Horizon Client. Lorsque l'option **Se connecter en tant qu'utilisateur actuel** est visible, les utilisateurs peuvent sélectionner ou désélectionner cette option et remplacer sa valeur par défaut. Lorsque l'option **Se connecter en tant qu'utilisateur actuel** est masquée, les utilisateurs ne peuvent pas remplacer sa valeur par défaut dans le menu **Options** d'Horizon Client. Vous pouvez spécifier la valeur par défaut de **Se connecter en tant qu'utilisateur actuel** en utilisant le paramètre de stratégie `Default value of the 'Log in as current user' checkbox`. Ce paramètre est activé par défaut. La valeur de Registre Windows équivalente est `LogInAsCurrentUser_Display`.
`Enable jump list integration`	X		Détermine si une liste de raccourcis doit s'afficher dans l'icône Horizon Client sur la barre des tâches des systèmes Windows 7 ou versions ultérieures. La liste de raccourcis permet aux utilisateurs de se connecter aux serveurs, postes de travail distants et applications publiées récents. Si Horizon Client est partagé, vous pouvez souhaiter que les utilisateurs ne voient pas les noms des applications publiées et postes de travail récents. Vous pouvez désactiver la liste de raccourcis en désactivant ce paramètre. Ce paramètre est activé par défaut. La valeur de Registre Windows équivalente est `EnableJumplist`.
`Enable SSL encrypted framework channel`	X	X	Détermine si TLS est activé pour les postes de travail distants View 5.0 et version antérieure. Avant View 5.0, les données envoyées au poste de travail distant via le port TCP 32111 n'étaient pas chiffrées. ■ **Activer** : active TLS, mais autorise le retour à la connexion non chiffrée précédente si le poste de travail distant ne prend pas en charge le protocole TLS. Par exemple, les postes de travail distants 5.0 et versions antérieures ne prennent pas en charge le protocole TLS. **Activer** est le paramètre par défaut. ■ **Désactiver** : désactive TLS. Ce peut être utile pour le débogage ou si le canal n'est pas configuré en tunnel et peut par la suite faire l'objet d'une optimisation par un produit d'accélération du réseau WAN. ■ **Appliquer** : active TLS et refuse de vous connecter à des postes de travail distants qui ne disposent pas de prise en charge du protocole TLS . La valeur de Registre Windows équivalente est `EnableTicketSSLAuth`.

Tableau 3-5. Modèle de configuration d'Horizon Client : paramètres de sécurité (suite)

Paramètre	Ordinateur	Utilisateur	Description
`Configures SSL protocols and cryptographic algorithms`	X	X	Configure la liste de chiffrements afin de limiter l'utilisation de certains protocoles et algorithmes de chiffrement avant l'établissement d'une connexion TLS chiffrée. La liste de chiffrements est composée d'une ou de plusieurs chaînes de chiffrement séparées par deux points. La chaîne de chiffrement est sensible à la casse. La valeur par défaut est **TLSv1.1:TLSv1.2:!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES** Cette chaîne de chiffrement signifie que TLS v1.1 et TLS v1.2 sont activés et que SSL v.2.0, SSL v3.0 et TLS v1.0 sont désactivés. SSL v2.0, SSL v3.0 et TLS v1.0 ne sont plus les protocoles approuvés et sont définitivement désactivés. Les suites de chiffrement utilisent ECDHE, ECDH et RSA avec AES 128 bits ou 256 bits. Le mode GCM est préféré. Pour plus d'informations, reportez-vous à http://www.openssl.org/docs/apps/ciphers.html. La valeur de Registre Windows équivalente est `SSLCipherList`.
`Enable Single Sign-On for smart card authentication`	X		Détermine si l'authentification unique est activée pour l'authentification par carte à puce. Lorsque l'authentification unique est activée, Horizon Client stocke le code PIN de carte à puce chiffré dans la mémoire temporaire avant de l'envoyer au Serveur de connexion. Lorsque l'authentification unique est désactivée, Horizon Client n'affiche pas de boîte de dialogue de code PIN personnalisée. La valeur de Registre Windows équivalente est `EnableSmartCardSSO`.

Tableau 3-5. Modèle de configuration d'Horizon Client : paramètres de sécurité (suite)

Paramètre	Ordinateur	Utilisateur	Description
`Ignore certificate revocation problems`	X	X	Détermine si les erreurs associées à un certificat de serveur révoqué sont ignorées. Ces erreurs se produisent lorsque le certificat que le serveur envoie a été révoqué ou que le client ne peut pas vérifier l'état de révocation du certificat. Ce paramètre est désactivé par défaut. **Note** Lorsque ce paramètre est activé, le client peut uniquement utiliser une URL mise en cache lors de la vérification du certificat de serveur. Les types d'informations d'URL mises en cache peuvent être le point de distribution CRL (CDP) et l'accès aux informations de l'autorité (méthodes d'accès à l'émetteur d'autorité de certification et OCSP).
`Unlock remote sessions when the client machine is unlocked`	X	X	Détermine si la fonctionnalité Déverrouillage récursif est activée. Cette fonctionnalité déverrouille toutes les sessions distantes après que la machine cliente a été déverrouillée. Cette fonctionnalité s'applique uniquement après qu'un utilisateur s'est connecté au serveur en tant qu'utilisateur actuel. Ce paramètre est activé par défaut.

Les paramètres suivants s'affichent dans le dossier **Configuration de VMware Horizon Client > Paramètres de sécurité > Paramètres NTLM** dans l'Éditeur de gestion de stratégie de groupe.

Tableau 3-6. Modèle de configuration d'Horizon Client : Paramètres de sécurité, Paramètres d'authentification NTLM

Paramètre	Ordinateur	Utilisateur	Description
`Allow NTLM Authentication`	X		Lorsque ce paramètre est activé, l'authentification NTLM est autorisée avec la fonctionnalité **Se connecter en tant qu'utilisateur actuel**. Lorsque ce paramètre est désactivé, l'authentification NTLM n'est utilisée pour aucun serveur. Lorsque ce paramètre est activé, vous pouvez sélectionner **Oui** ou **Aucun** dans le menu déroulant **Autoriser le recours de Kerberos à NTLM**. ■ Si vous sélectionnez **Oui**, vous pouvez utiliser l'authentification NTLM chaque fois que le client ne parvient pas à récupérer un ticket Kerberos pour le serveur. ■ Si vous sélectionnez **Aucun**, l'authentification NTLM n'est autorisée que pour les serveurs répertoriés dans le paramètre de stratégie de groupe **Toujours utiliser NTLM pour les serveurs**. Lorsque ce paramètre n'est pas configuré, l'authentification NTLM est autorisée pour les serveurs répertoriés dans le paramètre de stratégie de groupe **Toujours utiliser NTLM pour les serveurs**. Pour utiliser l'authentification NTLM, le certificat SSL du serveur doit être valide et les stratégies Windows ne doivent pas limiter l'utilisation de NTLM. Pour plus d'informations sur la configuration du recours de Kerberos à NTLM dans une instance du Serveur de connexion, reportez-vous à la section « Utilisation de la fonctionnalité Se connecter en tant qu'utilisateur actuel disponible avec une instance d'Horizon Client basée sur Windows » dans le document *Administration de VMware Horizon Console*.
`Always use NTLM for servers`	X		Lorsque ce paramètre est activé, l'option **Se connecter en tant qu'utilisateur actuel** utilise toujours l'authentification NTLM pour les serveurs répertoriés. Pour créer la liste de serveurs, cliquez sur **Afficher** et entrez le nom du serveur dans la colonne **Valeur**. Le format d'attribution de nom des serveurs est le nom de domaine complet (FQDN).

Paramètres RDP des objets de stratégie de groupe (GPO) des clients

Lorsque vous utilisez le protocole d'affichage RDP de Microsoft, vous pouvez configurer des stratégies de groupe pour des options telles que la redirection des périphériques audio, des imprimantes, des ports ou d'autres périphériques.

Le tableau suivant décrit les paramètres RDP (Remote Desktop Protocol) situés dans le fichier de modèle ADMX de configuration d'Horizon Client. Tous les paramètres RDP sont des paramètres de Configuration d'utilisateur. Les paramètres sont affichés dans le dossier **Configuration de VMware Horizon Client > Paramètres RDP** dans l'Éditeur de gestion de stratégie de groupe.

Tableau 3-7. Horizon Client Modèle d'administration de configuration : paramètres RDP

Paramètre	Description
`Audio redirection`	Détermine si les informations audio lues sur le poste de travail distant doivent être redirigées. Sélectionnez l'un des paramètres suivants : ■ **Désactiver le son** : le son est désactivé. ■ **Lire sur la machine virtuelle (nécessaire pour la prise en charge d'USB VoIP)** : les données audio sont lues sur le poste de travail distant. Ce paramètre requiert un périphérique audio USB partagé pour que le client reçoive le son. ■ **Rediriger vers le client** : les sons sont redirigés vers le client. Ce paramètre est le mode par défaut. Ce paramètre ne s'applique qu'à l'audio RDP. Les sons redirigés via MMR sont lus sur le client.
`Enable audio capture redirection`	Détermine si le périphérique d'entrée audio par défaut est redirigé du client vers la session distante. Lorsque ce paramètre est activé, le périphérique d'enregistrement audio sur le client s'affiche sur le poste de travail distant et peut enregistrer une entrée audio. Le paramètre par défaut est désactivé.
`Bitmap cache file size in` *unit* `for` *number* `bpp bitmaps`	Spécifie la taille du cache bitmap, en kilo-octets ou en mégaoctets, à utiliser pour les paramètres de couleur bitmap d'un nombre de bits par pixel (bpp) spécifique. Des versions séparées de ce paramètre sont fournies pour les combinaisons unité/bpp suivantes : ■ Mo/8 bpp ■ Mo/16 bpp ■ Mo/24 bpp ■ Mo/32 bpp
`In-memory bitmap cache size in KB for 8bpp bitmaps`	Spécifie la taille, en kilo-octets, du cache d'images bitmap de la RAM à utiliser pour le paramètre de couleur à 8 bits par pixel. Si ScaleBitmapCachesByBPP a la valeur true (par défaut), cette taille de cache est multipliée par le nombre d'octets par pixel pour déterminer la taille réelle du cache de la RAM. Lorsque ce paramètre est activé, entrez une taille en kilo-octets.
`Bitmap caching/cache persistence active`	Détermine si la mise en cache permanente des bitmaps est utilisée (active). La mise en cache permanente des bitmaps peut améliorer les performances de votre ordinateur mais requiert plus d'espace disque.
`Color depth`	Spécifie l'intensité des couleurs du poste de travail distant. Sélectionnez l'un des paramètres disponibles : ■ 8 bits ■ 15 bits ■ 16 bits ■ 24 bits ■ 32 bits
`Cursor shadow`	Détermine si une ombre doit s'afficher sous le curseur sur le poste de travail distant.
`Desktop background`	Détermine si l'arrière-plan du poste de travail doit être visible lorsque des clients se connectent à un poste de travail distant.

Tableau 3-7. Horizon Client Modèle d'administration de configuration : paramètres RDP (suite)

Paramètre	Description
`Desktop composition`	Détermine si la composition de poste de travail est activée sur le poste de travail distant. Lorsque la composition de poste de travail est activée, les fenêtres individuelles ne se dessinent plus sur l'écran ou sur le périphérique d'affichage principal comme c'était le cas dans les précédentes versions de Microsoft Windows. Le dessin est redirigé vers des surfaces non affichées à l'écran, en mémoire vidéo, qui sont ensuite rendues sous la forme d'une image de poste de travail et représentées à l'écran.
`Enable compression`	Détermine si les données RDP sont compressées. Ce paramètre est activé par défaut.
`Enable RDP Auto-Reconnect`	Détermine si le composant client RDP doit tenter de se reconnecter à un poste de travail distant après un échec de connexion du protocole RDP. Ce paramètre n'a aucun effet si l'option **Utiliser une connexion par tunnel sécurisé vers le poste de travail** est activée dans Horizon Console. Ce paramètre est désactivé par défaut.
`Font smoothing`	Détermine si l'anticrénelage est appliqué aux polices sur le poste de travail distant.
`Menu and window animation`	Détermine si l'animation des menus et des fenêtres doit être activée lorsque des clients se connectent à un poste de travail distant.
`Redirect clipboard`	Détermine si les informations locales du Presse-papiers doivent être redirigées lorsque des clients se connectent au poste de travail distant.
`Redirect drives`	Détermine si les lecteurs de disques locaux doivent être redirigés lorsque des clients se connectent au poste de travail distant. Par défaut, les lecteurs locaux sont redirigés. L'activation de ce paramètre, ou le laisser non configuré, permet de copier des données entre le lecteur redirigé sur le poste de travail distant et le lecteur sur l'ordinateur client. Désactivez ce paramètre si autoriser des données à passer du poste de travail distant à des ordinateurs clients d'utilisateurs représente un risque de sécurité potentiel dans votre déploiement. Une autre approche consiste à désactiver la redirection de dossier dans la machine virtuelle de poste de travail distant en activant le paramètre de stratégie de groupe de Microsoft Windows, `Do not allow drive redirection`. Le paramètre `Redirect drives` ne s'applique qu'à RDP.
`Redirect printers`	Détermine si les imprimantes locales doivent être redirigées lorsque des clients se connectent au poste de travail distant.
`Redirect serial ports`	Détermine si les ports COM locaux doivent être redirigés lorsque des clients se connectent au poste de travail distant.
`Redirect smart cards`	Détermine si les cartes à puce locales doivent être redirigées lorsque des clients se connectent au poste de travail distant. **Note** Ce paramètre s'applique aux connexions RDP et PCoIP.
`Redirect supported plug-and-play devices`	Détermine si les périphériques locaux de point de vente et Plug-and-Play doivent être redirigés lorsque des clients se connectent au poste de travail distant. Ce comportement est différent de la redirection gérée par le composant de redirection USB de l'agent.

Tableau 3-7. Horizon Client Modèle d'administration de configuration : paramètres RDP (suite)

Paramètre	Description
`Shadow bitmaps`	Détermine si les bitmaps sont ombrés. Ce paramètre n'a pas d'effet en plein écran.
`Show contents of window while dragging`	Détermine si le contenu des dossiers s'affiche lorsqu'un utilisateur les fait glisser vers un nouvel emplacement.
`Themes`	Détermine si des thèmes doivent s'afficher lorsque des clients se connectent à un poste de travail distant.
`Windows key combination redirection`	Détermine où les combinaisons de clés Windows sont appliquées. Ce paramètre vous permet d'envoyer des combinaisons de clés à la machine virtuelle distante ou d'appliquer des combinaisons de clés localement. Les combinaisons de touches sont appliquées localement par défaut.
`Enable Credential Security Service Provider`	Spécifie si la connexion Bureau à distance doit utiliser l'authentification au niveau du réseau (NLA). Si le système d'exploitation invité nécessite l'authentification au niveau du réseau pour les connexions de poste de travail distant, vous devez activer ce paramètre de sorte qu'Horizon Client soit en mesure de se connecter au poste de travail distant. En plus d'activer ce paramètre, vous devez également vérifier que les conditions suivantes sont satisfaites : ■ Le client et le système d'exploitation client prennent en charge la NLA. ■ Les connexions client directes sont activées pour l'instance du Serveur de connexion. Les connexions par tunnel ne sont pas prises en charge avec la NLA.

Paramètres généraux des objets de stratégie de groupe (GPO) de clients

Les paramètres incluent les options de proxy, de transfert de fuseau horaire, d'accélération multimédia et d'autres paramètres d'affichage.

Paramètres généraux

Le tableau suivant décrit les paramètres généraux figurant dans le fichier de modèle d'administration ADMX de configuration d'Horizon Client. Les paramètres généraux incluent des paramètres de Configuration d'ordinateur et de Configuration d'utilisateur. Le paramètre de Configuration d'utilisateur remplace le paramètre de Configuration d'ordinateur équivalent. Les paramètres se trouvent dans le dossier **Configuration de VMware Horizon Client** de l'éditeur de gestion de stratégie de groupe.

Tableau 3-8. Modèle de configuration d'Horizon Client : paramètres généraux

Paramètre	Ordinateur	Utilisateur	Description
`Allow Blast connections to use operating system proxy settings`	X		Configure l'utilisation du serveur proxy pour les connexions VMware Blast. Lorsque ce paramètre est activé, VMware Blast peut se connecter via un serveur proxy. Lorsque ce paramètre est désactivé, VMware Blast ne peut pas utiliser un serveur proxy. Lorsque ce paramètre n'est pas configuré (par défaut), les utilisateurs peuvent configurer si les connexions VMware Blast peuvent utiliser un serveur proxy dans l'interface utilisateur d'Horizon Client. Reportez-vous à Configurer des options VMware Blast.
`Allow data sharing`	X		Lorsque ce paramètre est activé, le paramètre de mode de partage de données dans l'interface utilisateur d'Horizon Client est défini sur Activé et les utilisateurs finaux ne peuvent pas modifier le paramètre. Lorsque ce paramètre est désactivé, le paramètre de mode de partage de données dans l'interface utilisateur d'Horizon Client est défini sur Désactivé et les utilisateurs finaux ne peuvent pas modifier le paramètre. Lorsque ce paramètre n'est pas configuré (par défaut), les utilisateurs finaux peuvent modifier le paramètre de mode de partage des données dans l'interface utilisateur d'Horizon Client.
`Allow display scaling`	X	X	Lorsque ce paramètre est activé, la fonctionnalité de mise à l'échelle de l'affichage est activée pour l'ensemble des postes de travail distants et des applications publiées. Lorsque ce paramètre est désactivé, la fonctionnalité de mise à l'échelle de l'affichage est désactivée pour l'ensemble des postes de travail distants et des applications publiées. Si ce paramètre n'est pas configuré (par défaut), les utilisateurs finaux peuvent activer et désactiver la mise à l'échelle de l'affichage dans l'interface utilisateur d'Horizon Client. Vous pouvez également masquer la préférence de mise à l'échelle de l'affichage dans l'interface utilisateur d'Horizon Client en activant le paramètre de stratégie de groupe **Taille d'invité verrouillée**. Pour plus d'informations, reportez-vous à la section Paramètres de définition de scripts des objets de stratégie de groupe (GPO) des clients.
`Allow H.264 Decoding`	X		Configure le décodage H.264 pour le protocole VMware Blast. Lorsque ce paramètre est activé, le décodage H.264 devient l'option préférée. Lorsque ce paramètre est désactivé, le décodage H.264 n'est jamais utilisé. Lorsque ce paramètre n'est pas configuré, les utilisateurs peuvent choisir d'activer ou non le décodage H.264. Reportez-vous à Configurer des options VMware Blast.

Tableau 3-8. Modèle de configuration d'Horizon Client : paramètres généraux (suite)

Paramètre	Ordinateur	Utilisateur	Description
Allow H.264 high color accuracy	X		Configure le mode de haute précision couleurs pour H.264. Ce paramètre prend effet uniquement si le décodage H.264 est activé. Lorsque ce paramètre n'est pas configuré, les utilisateurs peuvent choisir d'activer ou non le mode de haute précision couleurs. Reportez-vous à Configurer des options VMware Blast.
Allow HEVC Decoding	X		Configure le décodage HEVC (également appelé H.265) pour le protocole VMware Blast. Lorsque ce paramètre est activé, le décodage HEVC devient l'option préférée. Lorsque ce paramètre est désactivé, le décodage HEVC n'est jamais utilisé. Lorsque ce paramètre n'est pas configuré, les utilisateurs peuvent choisir d'activer ou non le décodage HEVC. Reportez-vous à Configurer des options VMware Blast.
Allow user to skip Horizon Client update	X		Spécifie si les utilisateurs peuvent cliquer sur le bouton **Ignorer** dans la fenêtre de mise à jour d'Horizon Client. Si les utilisateurs cliquent sur **Ignorer**, ils ne voient pas d'autres notifications de mise à jour tant que la version suivante d'Horizon Client n'est pas disponible.
Always hide the remote floating language (IME) bar for Hosted Apps	X	X	Force la barre de langue flottante à disparaître pour les sessions d'application. Lorsque ce paramètre est activé, la barre de langue flottante n'est jamais affichée dans une session d'application publiée, que la fonctionnalité IME local soit activée ou non. Lorsque ce paramètre est désactivé, la barre de langue flottante n'est affichée que si la fonctionnalité IME local est désactivée. Ce paramètre est désactivé par défaut.
Always on top		X	Détermine si la fenêtre Horizon Client doit toujours rester au premier plan. L'activation de ce paramètre empêche la barre des tâches de Windows de s'afficher sur la fenêtre Horizon Client en plein écran. Ce paramètre est désactivé par défaut.
Automatic input focus in a virtual desktop window	X	X	Lorsque ce paramètre est activé, Horizon Client envoie automatiquement une entrée au poste de travail distant lorsqu'un utilisateur met le poste de travail distant au premier plan. En d'autres termes, le focus n'est pas dans le cadre de la fenêtre et l'utilisateur n'a pas besoin de cliquer dans la fenêtre du poste de travail distant pour déplacer le focus.
Automatically check for updates	X		Spécifie s'il faut rechercher automatiquement les mises à jour logicielles Horizon Client. Ce paramètre contrôle la case à cocher **Rechercher les mises à jour et afficher la notification de badge** dans la fenêtre de mise à jour d'Horizon Client. Ce paramètre est activé par défaut.

Tableau 3-8. Modèle de configuration d'Horizon Client : paramètres généraux (suite)

Paramètre	Ordinateur	Utilisateur	Description
`Automatically install shortcuts when configured on the Horizon server`		X	Lorsque des raccourcis d'application publiée et de poste de travail sont configurés sur une instance du Serveur de connexion, ce paramètre spécifie comment et si les raccourcis sont installés sur les machines clientes lorsque les utilisateurs se connectent au serveur. Lorsque ce paramètre est activé, les raccourcis sont installés sur les machines clientes. Les utilisateurs ne sont pas invités à installer les raccourcis. Lorsque ce paramètre est désactivé, les raccourcis ne sont jamais installés sur des machines clientes. Les utilisateurs ne sont pas invités à installer les raccourcis. Les utilisateurs sont invités à installer les raccourcis par défaut.
`Automatically synchronize the keypad, scroll and caps lock keys`	X		Lorsque ce paramètre est activé, les états de basculement des touches Verr Num, Arrêt défil et Verr. maj sont synchronisés depuis le périphérique client vers un poste de travail distant. Dans Horizon Client, la case **Synchroniser automatiquement le pavé numérique, les touches de défilement et de verrouillage des majuscules** est cochée et le paramètre est grisé. Lorsque ce paramètre est désactivé, les états de basculement de touche de verrouillage sont synchronisés du poste de travail distant vers le périphérique client. Dans Horizon Client, la case **Synchroniser automatiquement le pavé numérique, les touches de défilement et de verrouillage des majuscules** est décochée et le paramètre est grisé. Lorsque ce paramètre est activé ou désactivé, les utilisateurs ne peuvent pas modifier le paramètre **Synchroniser automatiquement le pavé numérique, les touches de défilement et de verrouillage des majuscules** dans Horizon Client. Lorsque ce paramètre n'est pas configuré, un utilisateur peut activer ou désactiver la synchronisation de la touche de verrouillage pour un poste de travail distant en configurant le paramètre **Synchroniser automatiquement le pavé numérique, les touches de défilement et de verrouillage des majuscules** dans Horizon Client. Reportez-vous à Configurer la synchronisation des touches de verrouillage. Ce paramètre n'est pas configuré par défaut.
`Block multiple Horizon Client instances per Windows session`	X		Empêche l'utilisateur de démarrer plusieurs instances d'Horizon Client pendant une session Windows. Lorsque ce paramètre est activé, Horizon Client s'exécute en mode d'instance unique et un utilisateur ne peut pas démarrer plusieurs instances de Horizon Client dans une session Windows. Lorsque ce paramètre est désactivé, un utilisateur peut lancer plusieurs instances d'Horizon Client dans une session Windows. Ce paramètre est désactivé par défaut.

Tableau 3-8. Modèle de configuration d'Horizon Client : paramètres généraux (suite)

Paramètre	Ordinateur	Utilisateur	Description
`Configure maximum latency for mouse coalescing`	X		Définit la latence maximale autorisée, en millisecondes, lors de la fusion des événements de déplacement de la souris. Les valeurs valides sont comprises entre 0 et 50. La fonctionnalité est désactivée si la valeur est égale à 0. La fusion des événements de déplacement de la souris peut réduire l'utilisation de la bande passante client à agent, mais peut potentiellement ajouter une latence mineure au déplacement de la souris. Ce paramètre est désactivé par défaut.
`Custom error screen footer`	X		Permet d'ajouter le texte d'aide personnalisé au bas de tous les messages d'erreur d'Horizon Client. Vous devez fournir le texte d'aide dans un fichier de texte brut (`.txt`) sur le système client local. Le fichier texte peut contenir jusqu'à 2 048 caractères, y compris des caractères de contrôle. Les encodages ANSI et Unicode sont tous deux pris en charge. Lorsque ce paramètre est activé, vous spécifiez le chemin d'accès complet au fichier qui contient le texte d'aide personnalisé dans la zone de texte fournie, par exemple, `C:\myDocs\errorFooter.txt`. Ce paramètre est désactivé par défaut.
`Default value of the "Hide the selector after launching an item" check box`	X	X	Définit si la case **Masquer le sélecteur après le lancement d'un élément** est cochée par défaut. Ce paramètre est désactivé par défaut.
`Disable desktop disconnect messages`	X	X	Indique si les messages qui s'affichent généralement lors de la déconnexion du poste de travail distant sont désactivés. Ces messages s'affichent par défaut.
`Disable sharing files and folders`		X	Spécifie si la fonctionnalité de redirection du lecteur client est disponible dans Horizon Client. Lorsque ce paramètre est activé, toute la fonctionnalité de redirection du lecteur client est désactivée dans Horizon Client, notamment la capacité d'ouvrir des fichiers locaux avec des applications publiées. De plus, les éléments suivants sont masqués dans l'interface utilisateur d'Horizon Client : ■ Partage de volet dans la boîte de dialogue Paramètres. ■ Élément **Partager les dossiers** dans le menu **Option** d'un poste de travail distant. ■ Élément **Partage** pour Horizon Client dans la barre d'état système. ■ Boîte de dialogue Partage qui s'affiche la première fois que vous vous connectez à une application ou à un poste de travail distant après vous être connecté à un serveur. Lorsque ce paramètre est désactivé, la fonctionnalité de redirection du lecteur client est entièrement opérationnelle. Ce paramètre est désactivé par défaut.

Tableau 3-8. Modèle de configuration d'Horizon Client : paramètres généraux (suite)

Paramètre	Ordinateur	Utilisateur	Description
`Disable time zone forwarding`	X		Détermine si la synchronisation de fuseau horaire entre le poste de travail distant et le client connecté doit être désactivée.
`Disable toast notifications`	X	X	Détermine s'il faut désactiver les notifications toast dans Horizon Client. Activez ce paramètre si vous ne voulez pas que l'utilisateur voie des notifications de toast dans le coin de l'écran. **Note** Si vous activez ce paramètre, l'utilisateur ne voit pas d'avertissement de 5 minutes lorsque la fonction Session Timeout (Délai d'expiration de la session) est active.
`Disallow passing through client information in a nested session`	X		Spécifie s'il faut empêcher Horizon Client de transférer les informations du client dans une session imbriquée. Lorsqu'il est activé, si Horizon Client est en cours d'exécution dans une session à distance, il envoie les informations physiques réelles du client au lieu des informations du périphérique de machine virtuelle. Ce paramètre s'applique aux informations du client suivantes : domaine et nom du périphérique, type de client, adresse IP et adresse MAC. Ce paramètre est désactivé par défaut, ce qui signifie que le transfert d'informations du client dans une session imbriquée est autorisé.
`Display modifier function key`	X	X	Spécifie la touche de fonction et de modification du changement d'affichage sur laquelle un utilisateur peut appuyer qui, lors de la saisie et de l'envoi de la saisie dans une session de poste de travail distant utilisant PCoIP ou VMware Blast, modifie la configuration de l'affichage sur la machine cliente. Lorsque ce paramètre n'est pas configuré (par défaut), l'utilisateur final doit utiliser la souris pour annuler la saisie du poste de travail distant, puis appuyer sur la touche du logo Windows + P pour sélectionner un mode d'affichage de présentation. Ce paramètre ne s'applique pas aux sessions de l'application publiée.

Tableau 3-8. Modèle de configuration d'Horizon Client : paramètres généraux (suite)

Paramètre	Ordinateur	Utilisateur	Description
`Disable opening local files in hosted applications`		X	Spécifie si Horizon Client enregistre des gestionnaires locaux pour les extensions de fichier que les applications hébergées prennent en charge. Lorsque ce paramètre est activé, Horizon Client n'enregistre aucun gestionnaire d'extension de fichier et n'autorise pas l'utilisateur à remplacer le paramètre. Lorsque ce paramètre est désactivé, Horizon Client enregistre toujours les gestionnaires d'extension de fichier. Par défaut, les gestionnaires d'extension de fichier sont enregistrés, mais les utilisateurs peuvent désactiver la fonctionnalité dans l'interface utilisateur d'Horizon Client en utilisant le paramètre **Activer la fonction permettant d'ouvrir un fichier local avec une application distante depuis le système de fichiers local** sur le volet Partage dans la boîte de dialogue Paramètres. Pour plus d'informations, reportez-vous à la section Partager des lecteurs et des dossiers locaux. Ce paramètre est désactivé par défaut.
`Don't check monitor alignment on spanning`		X	Par défaut, le poste de travail client ne s'étend pas sur plusieurs écrans si la combinaison de ces derniers ne forme pas un rectangle exact lorsqu'ils sont combinés. Activez ce paramètre pour remplacer la valeur par défaut. Ce paramètre est désactivé par défaut.
`Enable multi-media acceleration`		X	Détermine si la redirection multimédia (MMR) est activée sur le client. MMR ne fonctionne pas correctement si le matériel d'affichage vidéo d'Horizon Client ne prend pas en charge la superposition.
`Enable relative mouse`	X	X	Active la souris relative lors de l'utilisation du protocole d'affichage PCoIP. Le mode de souris relative améliore le comportement de la souris pour certaines applications graphiques et certains jeux. Si le poste de travail distant ne prend pas en charge la souris relative, ce paramètre ne sera pas utilisé. Ce paramètre est désactivé par défaut.
`Enable the shade`		X	Détermine si le menu Ombre situé en haut de la fenêtre Horizon Client doit être visible. Ce paramètre est activé par défaut. **Note** La barre de menu ombre est désactivée par défaut pour le mode kiosque.
`Enable Horizon Client online update`	X		Active la fonctionnalité de mise à jour en ligne. Ce paramètre est activé par défaut. **Note** Vous pouvez également désactiver la fonctionnalité de mise à jour en ligne en définissant la propriété `AUTO_UPDATE_ENABLED` sur 0 lorsque vous installez Horizon Client à partir de la ligne de commande. Pour plus d'informations, reportez-vous à la section Propriétés d'installation d'Horizon Client.

Tableau 3-8. Modèle de configuration d'Horizon Client : paramètres généraux (suite)

Paramètre	Ordinateur	Utilisateur	Description
`Hide items in application context menu`	X	X	Utilisez ce paramètre pour masquer des éléments dans le menu contextuel qui s'affiche lorsque vous cliquez avec le bouton droit sur une application publiée dans la fenêtre de sélection des postes de travail et applications. Lorsque ce paramètre est activé, vous pouvez configurer les options suivantes : ■ **Masquer les paramètres** : sélectionnez **Oui** pour masquer l'élément **Paramètres** dans le menu contextuel. ■ **Masquer Créer un raccourci sur le Bureau** : sélectionnez **Oui** pour masquer l'élément **Créer un raccourci sur le Bureau** dans le menu contextuel. ■ **Masquer Ajouter au menu Démarrer** : sélectionnez **Oui** pour masquer l'élément **Ajouter au menu Démarrer** dans le menu contextuel. ■ **Masquer Marquer comme favori** : sélectionnez **Oui** pour masquer l'élément **Marquer comme favori** dans le menu contextuel. Ce paramètre est désactivé par défaut.
`Hide items in desktop context menu`	X	X	Utilisez ce paramètre pour masquer des éléments dans le menu contextuel qui s'affiche lorsque vous cliquez avec le bouton droit sur un poste de travail distant dans la fenêtre de sélection des postes de travail et applications. Lorsque ce paramètre est activé, vous pouvez configurer les options suivantes : ■ **Masquer Réinitialiser le poste de travail** : sélectionnez **Oui** pour masquer l'élément **Réinitialiser le poste de travail** dans le menu contextuel. ■ **Masquer Redémarrer le poste de travail** : sélectionnez **Oui** pour masquer l'élément **Redémarrer le poste de travail** dans le menu contextuel. ■ **Masquer Afficher** : sélectionnez **Oui** pour masquer l'élément **Afficher** dans le menu contextuel. ■ **Masquer les paramètres** : sélectionnez **Oui** pour masquer l'élément **Paramètres** dans le menu contextuel. ■ **Masquer Créer un raccourci sur le Bureau** : sélectionnez **Oui** pour masquer l'élément **Créer un raccourci sur le Bureau** dans le menu contextuel. ■ **Masquer Ajouter au menu Démarrer** : sélectionnez **Oui** pour masquer l'élément **Ajouter au menu Démarrer** dans le menu contextuel. ■ **Masquer Marquer comme favori** : sélectionnez **Oui** pour masquer l'élément **Marquer comme favori** dans le menu contextuel. Ce paramètre est désactivé par défaut.

Tableau 3-8. Modèle de configuration d'Horizon Client : paramètres généraux (suite)

Paramètre	Ordinateur	Utilisateur	Description
`Hide items in desktop toolbar`	X	X	Utilisez ce paramètre pour masquer des éléments sur la barre de menus dans une fenêtre du poste de travail distant. Lorsque ce paramètre est activé, vous pouvez configurer les options suivantes. ■ **Masquer l'aide** : sélectionnez **Oui** pour masquer l'élément **Aide** dans le menu **Options**. ■ **Masquer les informations de support** : sélectionnez **Oui** pour masquer l'élément **Informations de support** dans le menu **Options**. ■ **Masquer la souris relative activée** : sélectionnez **Oui** pour masquer l'élément **Activer la souris relative** dans le menu **Options**. ■ **Masquer les dossiers de partage** : sélectionnez **Oui** pour masquer l'élément **Dossiers de partage** dans le menu **Options**. ■ **Masquer Autoriser la mise à l'échelle de l'affichage** : sélectionnez **Oui** pour masquer l'élément **Autoriser la mise à l'échelle de l'affichage** dans le menu **Options**. ■ **Masquer Réinitialiser le poste de travail** : sélectionnez **Oui** pour masquer l'élément **Réinitialiser le poste de travail** dans le menu **Options**. ■ **Masquer Redémarrer le poste de travail** : sélectionnez **Oui** pour masquer l'élément **Redémarrer le poste de travail** dans le menu **Options**. ■ **Masquer Connecter le périphérique USB** : sélectionnez **Oui** pour masquer le menu **Connecter le périphérique USB** sur la barre de menus. Ce paramètre est désactivé par défaut.
`Hide items in system tray menu`	X	X	Utilisez ce paramètre pour masquer des éléments dans le menu contextuel qui s'affiche lorsque vous cliquez avec le bouton droit sur l'icône Horizon Client dans la barre d'état système sur le système client local. Lorsque ce paramètre est activé, vous pouvez configurer les options suivantes. ■ **Masquer le partage** : sélectionnez **Oui** pour masquer l'élément Horizon ClientPartage d'. ■ **Masquer les paramètres** : sélectionnez **Oui** pour masquer l'élément Horizon ClientParamètres d'. Ce paramètre est désactivé par défaut.

Tableau 3-8. Modèle de configuration d'Horizon Client : paramètres généraux (suite)

Paramètre	Ordinateur	Utilisateur	Description
`Hide items in the client toolbar menu`	X	X	Utilisez ce paramètre pour masquer des éléments dans la barre d'outils en haut de la fenêtre de sélection des postes de travail et applications. Lorsque ce paramètre est activé, vous pouvez configurer les options suivantes. ■ **Masquer la bascule des favoris** : sélectionnez **Oui** pour masquer l'icône **Afficher les favoris** (étoile). ■ **Masquer l'engrenage des paramètres** : sélectionnez **Oui** pour masquer l'icône **Paramètres** (engrenage). Ce paramètre est désactivé par défaut.
`Hotkey combination to grab input focus`	X	X	Configure une combinaison de touches d'accès rapide pour saisir le focus d'entrée pour la dernière session de poste de travail distant PCoIP ou VMware Blast utilisée. Une touche de raccourci se compose d'une ou de deux touches de modification et d'une touche de lettre. Lorsque ce paramètre est désactivé ou n'est pas configuré, l'utilisateur peut prendre le focus en cliquant à l'intérieur de la fenêtre du poste de travail. Ce paramètre n'est pas configuré par défaut.
`Hotkey combination to release input focus`	X	X	Configure une combinaison de touches d'accès rapide pour libérer le focus d'entrée à partir d'une session de poste de travail distant PCoIP ou VMware Blast. Une touche de raccourci se compose d'une ou de deux touches de modification et d'une touche de fonction. Lorsque la case **Réduire le poste de travail virtuel plein écran après avoir libéré le focus d'entrée** est cochée, les utilisateurs peuvent appuyer sur n'importe quelle touche de raccourci clavier configurée pour libérer le focus d'entrée (par exemple, Ctrl+Maj+F5) pour réduire la fenêtre du poste de travail distant lorsque celui-ci est en plein écran. Par défaut, Ctrl+Shift+F5 réduit la fenêtre du poste de travail distant lorsque le poste de travail est en mode plein écran sans configuration. Lorsque ce paramètre est désactivé ou n'est pas configuré, l'utilisateur peut libérer le focus en utilisant Ctrl+Alt ou en cliquant en dehors de la fenêtre du poste de travail distant. Ce paramètre n'est pas configuré par défaut.
`Pin the shade`		X	Détermine si l'épingle de l'ombre située en haut de la fenêtre Horizon Client doit être activée, de sorte que le masquage automatique de la barre de menus ne se produit pas. Ce paramètre est sans effet si l'ombre est désactivée. Ce paramètre est activé par défaut.

Tableau 3-8. Modèle de configuration d'Horizon Client : paramètres généraux (suite)

Paramètre	Ordinateur	Utilisateur	Description
`Save resolution and DPI to server`	X		Détermine si Horizon Client enregistre la résolution d'affichage personnalisée et les paramètres de mise à l'échelle de l'affichage sur le serveur. Pour plus d'informations sur la personnalisation des paramètres de résolution d'affichage et de mise à l'échelle de l'affichage d'un poste de travail distant, reportez-vous à la section Personnaliser la résolution et la mise à l'échelle de l'affichage pour un poste de travail distant. Lorsque ce paramètre est activé et que la résolution d'affichage ou la mise à l'échelle de l'affichage a été personnalisée pour un poste de travail distant, chaque fois qu'un utilisateur ouvre le poste de travail distant, les paramètres personnalisés sont appliqués automatiquement, quel que soit le périphérique client utilisé par l'utilisateur pour se connecter sur le poste de travail distant. Ce paramètre est désactivé par défaut.
`Tunnel proxy bypass address list`	X		Spécifie une liste d'adresses de tunnel. Le serveur proxy n'est pas utilisé pour ces adresses. Utilisez un point-virgule (;) pour séparer plusieurs entrées.
`Update message pop-up`	X		Spécifie s'il faut afficher automatiquement le message contextuel de mise à jour aux utilisateurs finaux lorsqu'une nouvelle version d'Horizon Client est disponible. Ce paramètre contrôle la case **Afficher le message contextuel en cas de mise à jour** dans la fenêtre de mise à jour d'Horizon Client. Ce paramètre est désactivé par défaut.
`URL for Horizon Client online help`	X		Spécifie une autre URL à partir de laquelle Horizon Client peut récupérer les pages d'aide. Ce paramètre est destiné à être utilisé dans des environnements qui ne peuvent pas récupérer le système d'aide hébergé à distance car ils ne disposent pas d'accès à Internet.
`URL for Horizon Client online update`	X		Spécifie une autre URL à partir de laquelle Horizon Client peut récupérer les mises à jour. Ce paramètre est conçu pour être utilisé dans un environnement qui définit son propre centre de mise à jour privé/personnel. S'il n'est pas activé, le serveur de mise à jour officiel de VMware est utilisé.

Paramètres USB des objets de stratégie de groupe (GPO) des clients

Vous pouvez définir des paramètres de stratégie USB pour Horizon Agent et Horizon Client. Lors de la connexion, Horizon Client télécharge les paramètres de stratégie USB depuis Horizon Agent et utilise ces paramètres, en même temps que les paramètres de stratégie USB d'Horizon Client, pour déterminer les terminaux qui sont disponibles pour la redirection depuis la machine hôte.

Paramètres de stratégie pour fractionner des périphériques USB composites

Le tableau suivant décrit chaque paramètre de fractionnement de périphériques USB composites situé dans le fichier de modèle d'administration ADMX pour la configuration d'Horizon Client. Les paramètres s'appliquent au niveau de l'ordinateur. Les paramètres depuis le GPO au niveau de l'ordinateur sont prioritaires sur le registre dans `HKLM\Software\Policies\VMware, Inc.\VMware VDM\Client\USB`. Les paramètres se trouvent dans le dossier **Configuration de VMware Horizon Client > Afficher la configuration USB** de l'éditeur de gestion de stratégie de groupe.

Pour plus d'informations sur l'utilisation de stratégies pour contrôler la redirection USB, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Tableau 3-9. Modèle de configuration d'Horizon Client : paramètres de fractionnement USB

Paramètre	Description
`Allow Auto Device Splitting`	Autorise le fractionnement automatique de périphériques USB composites. La valeur par défaut est indéfinie, ce qui correspond à **`false`**.
`Exclude Vid/Pid Device From Split`	Exclut un périphérique USB composite spécifié par des ID de fournisseur et de produit du fractionnement. Le format du paramètre est `vid-`*`xxx1`*`_pid-`*`yyy2`*`[;vid-`*`xxx2`*`_pid-`*`yyy2`*`]...` Vous devez spécifier des numéros d'ID au format hexadécimal. Vous pouvez utiliser le caractère générique (**`*`**) à la place de chiffres individuels dans un ID. Par exemple : **`vid-0781_pid-55**`** La valeur par défaut n'est pas définie.
`Split Vid/Pid Device`	Traite les composants d'un périphérique USB composite spécifiés par des ID de fournisseur et de produit en tant que périphériques séparés. Le format du paramètre est `vid-`*`xxxx`*`_pid-`*`yyyy`*`(exintf:`*`zz`*`[;exintf:`*`ww`*`])` Vous pouvez utiliser le mot-clé `exintf` pour exclure des composants de la redirection en spécifiant leur numéro d'interface. Vous devez spécifier les numéros d'ID au format hexadécimal et les numéros d'interface au format décimal en incluant les zéros à gauche. Vous pouvez utiliser le caractère générique (**`*`**) à la place de chiffres individuels dans un ID. Par exemple : **`vid-0781_pid-554c(exintf:01;exintf:02)`** **Note** Horizon n'inclut pas automatiquement les composants que vous n'avez pas explicitement exclus. Vous devez spécifier une règle de filtre telle que `Include Vid/Pid Device` pour inclure ces composants. La valeur par défaut n'est pas définie.

Paramètres de stratégie pour filtrer des périphériques USB

Le tableau suivant décrit les paramètres de stratégie dans le Horizon Clientmodèle de fichier ADMX de configuration pour le filtrage des périphériques USB. Les paramètres s'appliquent au niveau de l'ordinateur. Les paramètres depuis le GPO au niveau de l'ordinateur sont prioritaires sur le registre dans `HKLM\Software\Policies\VMware, Inc.\VMware VDM\Client\USB`.

Pour plus d'informations sur la configuration des paramètres de stratégie de filtre pour la redirection USB, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Tableau 3-10. Modèle de configuration d'Horizon Client : paramètres de filtrage USB

Paramètre	Description
`Allow Audio Input Devices`	Permet la redirection de périphériques d'entrée audio. La valeur par défaut est indéfinie, ce qui correspond à **`true`**. Ce paramètre se trouve dans le dossier **Configuration de VMware Horizon Client > Afficher la configuration USB** de l'éditeur de gestion de stratégie de groupe.
`Allow Audio Output Devices`	Permet la redirection de périphériques de sortie audio. La valeur par défaut est indéfinie, ce qui correspond à **`false`**. Ce paramètre se trouve dans le dossier **Configuration de VMware Horizon Client > Afficher la configuration USB** de l'éditeur de gestion de stratégie de groupe.
`Allow HID-Bootable`	Permet la redirection de périphériques d'entrée autres que des claviers et des souris qui sont disponibles au démarrage (ou périphériques démarrables par HID). La valeur par défaut est indéfinie, ce qui correspond à **`true`**. Ce paramètre se trouve dans le dossier **Configuration de VMware Horizon Client > Afficher la configuration USB** de l'éditeur de gestion de stratégie de groupe.
`Allow Device Descriptor Failsafe Behavior`	Autorise la redirection des périphériques même si Horizon Client ne parvient pas à obtenir les descripteurs de configuration/périphérique. Pour autoriser un périphérique même si config/desc échoue, incluez-le dans les filtres d'inclusion tels que `IncludeVidPid` ou `IncludePath`. La valeur par défaut est indéfinie, ce qui correspond à **`false`**. Ce paramètre se trouve dans le dossier **Configuration de VMware Horizon Client > Afficher la configuration USB > Paramètres non configurables par Agent** de l'éditeur de gestion de stratégie de groupe.
`Allow Other Input Devices`	Permet la redirection de périphériques d'entrée autres que des périphériques démarrables par HID ou des claviers avec périphériques de pointage intégrés. La valeur par défaut est indéfinie, ce qui correspond à **`true`**. Ce paramètre se trouve dans le dossier **Configuration de VMware Horizon Client > Afficher la configuration USB** de l'éditeur de gestion de stratégie de groupe.
`Allow Keyboard and Mouse Devices`	Permet la redirection de claviers avec périphériques de pointage intégrés (souris, Trackball ou pavé tactile). La valeur par défaut est indéfinie, ce qui correspond à **`false`**. Ce paramètre se trouve dans le dossier **Configuration de VMware Horizon Client > Afficher la configuration USB** de l'éditeur de gestion de stratégie de groupe.
`Allow Smart Cards`	Permet la redirection de périphériques à carte à puce. La valeur par défaut est indéfinie, ce qui correspond à **`false`**. Ce paramètre se trouve dans le dossier **Configuration de VMware Horizon Client > Afficher la configuration USB** de l'éditeur de gestion de stratégie de groupe.
`Allow Video Devices`	Permet la redirection de périphériques vidéo. La valeur par défaut est indéfinie, ce qui correspond à **`true`**. Ce paramètre se trouve dans le dossier **Configuration de VMware Horizon Client > Afficher la configuration USB** de l'éditeur de gestion de stratégie de groupe.

Tableau 3-10. Modèle de configuration d'Horizon Client : paramètres de filtrage USB (suite)

Paramètre	Description
`Disable Remote Configuration`	Désactive l'utilisation des paramètres de l'agent lors de l'exécution du filtrage des périphériques USB. La valeur par défaut est indéfinie, ce qui correspond à **`false`**. Ce paramètre se trouve dans le dossier **Configuration de VMware Horizon Client > Afficher la configuration USB > Paramètres non configurables par Agent** de l'éditeur de gestion de stratégie de groupe.
`Exclude All Devices`	Exclut tous les périphériques USB de la redirection. Si ce paramètre est défini sur **`true`**, vous pouvez utiliser d'autres paramètres de règle pour autoriser la redirection de périphériques spécifiques ou de familles de périphériques. Si ce paramètre est défini sur **`false`**, vous pouvez utiliser d'autres paramètres de règle pour empêcher la redirection de périphériques spécifiques ou de familles de périphériques. Si vous définissez la valeur de `Exclude All Devices` sur **`true`** sur l'agent, et si ce paramètre est transmis à Horizon Client, le paramètre de l'agent remplace celui d'Horizon Client. La valeur par défaut est indéfinie, ce qui correspond à **`false`**. Ce paramètre se trouve dans le dossier **Configuration de VMware Horizon Client > Afficher la configuration USB** de l'éditeur de gestion de stratégie de groupe.

`Exclude Automatically Connection Device Family`	Exclut des familles de périphériques de la transmission automatique. Utilisez la syntaxe suivante :
	`family-name[;...]`
	Par exemple :
	`storage;hid`

`Exclude Automatically Connection Vid/Pid Device`	Exclut de la transmission automatique des périphériques ayant des ID de fournisseur et de produit spécifiques. Utilisez la syntaxe suivante :
	`vid-xxxx_pid-xxxx|*[;...]`
	Par exemple :
	`vid-0781_pid-554c;vid-0781_pid-9999`

`Exclude Device Family`	Exclut des familles de périphériques de la redirection. Le format du paramètre est *nom_famille_1*[`;`*nom_famille_2*]... Par exemple : **`bluetooth;smart-card`** Si vous avez activé le fractionnement automatique de périphérique, Horizon examine la famille de périphériques de chaque interface d'un périphérique USB composite pour décider quelles interfaces doivent être exclues. Si vous avez désactivé le fractionnement automatique de périphérique, Horizon examine la famille de périphérique de l'ensemble du périphérique USB composite. La valeur par défaut n'est pas définie. Ce paramètre se trouve dans le dossier **Configuration de VMware Horizon Client > Afficher la configuration USB** de l'éditeur de gestion de stratégie de groupe.

Tableau 3-10. Modèle de configuration d'Horizon Client : paramètres de filtrage USB (suite)

Paramètre	Description
`Exclude Vid/Pid Device`	Exclut de la redirection des périphériques ayant des ID de fournisseur et de produit spécifiques. Le format du paramètre est `vid-`*xxx1*`_pid-`*yyy2*`[;vid-`*xxx2*`_pid-`*yyy2*`]`… Vous devez spécifier des numéros d'ID au format hexadécimal. Vous pouvez utiliser le caractère générique (*****) à la place de chiffres individuels dans un ID. Par exemple : **vid-0781_pid-****;vid-0561_pid-554c** La valeur par défaut n'est pas définie. Ce paramètre se trouve dans le dossier **Configuration de VMware Horizon Client > Afficher la configuration USB** de l'éditeur de gestion de stratégie de groupe.
`Exclude Path`	Exclut des périphériques dans des chemins de concentrateur ou de port spécifiés de la redirection. Le format du paramètre est `bus-`*x1*`[/`*y1*`]…/port-`*z1*`[;bus-`*x2*`[/`*y2*`]…/port-`*z2*`]`… Vous devez spécifier des numéros de bus et de port au format hexadécimal. Vous ne pouvez pas utiliser le caractère générique dans les chemins. Par exemple : **bus-1/2/3_port-02;bus-1/1/1/4_port-ff** La valeur par défaut n'est pas définie. Ce paramètre se trouve dans le dossier **Configuration de VMware Horizon Client > Afficher la configuration USB > Paramètres non configurables par Agent** de l'éditeur de gestion de stratégie de groupe.
`Include Device Family`	Inclut des familles de périphériques pouvant être redirigées. Le format du paramètre est *nom_famille_1*`[;`*nom_famille_2*`]`… Par exemple : **storage** La valeur par défaut n'est pas définie. Ce paramètre se trouve dans le dossier **Configuration de VMware Horizon Client > Afficher la configuration USB** de l'éditeur de gestion de stratégie de groupe.
`Include Path`	Inclut des périphériques dans des chemins de concentrateur ou de port spécifiés pouvant être redirigés. Le format du paramètre est `bus-`*x1*`[/`*y1*`]…/port-`*z1*`[;bus-`*x2*`[/`*y2*`]…/port-`*z2*`]`… Vous devez spécifier des numéros de bus et de port au format hexadécimal. Vous ne pouvez pas utiliser le caractère générique dans les chemins. Par exemple : **bus-1/2_port-02;bus-1/7/1/4_port-0f** La valeur par défaut n'est pas définie. Ce paramètre se trouve dans le dossier **Configuration de VMware Horizon Client > Afficher la configuration USB > Paramètres non configurables par Agent** de l'éditeur de gestion de stratégie de groupe.
`Include Vid/Pid Device`	Spécifie les périphériques USB qui ont un ID de fournisseur et de produit spécifié pouvant être redirigé. Le format du paramètre est `vid-`*xxx1*`_pid-`*yyy2*`[;vid-`*xxx2*`_pid-`*yyy2*`]`… Vous devez spécifier des numéros d'ID au format hexadécimal. Vous pouvez utiliser le caractère générique (*****) à la place de chiffres individuels dans un ID. Par exemple : **vid-0561_pid-554c** La valeur par défaut n'est pas définie. Ce paramètre se trouve dans le dossier **Configuration de VMware Horizon Client > Afficher la configuration USB** de l'éditeur de gestion de stratégie de groupe.

Considérations pour les sessions imbriquées

Dans un scénario en mode imbriqué ou à deux tronçons, un utilisateur se connecte à partir de son système client physique à un poste de travail distant, démarre Horizon Client au sein du poste de travail distant (la session imbriquée) et se connecte à un autre poste de travail distant. Pour que le périphérique fonctionne comme prévu dans la session imbriquée, vous devez configurer les paramètres de stratégie USB de la même manière sur la machine cliente physique et dans la session imbriquée.

Paramètres de redirection de VMware Browser pour les objets de stratégie de groupe des clients

Vous pouvez configurer des paramètres de stratégie de groupe pour la fonctionnalité de redirection de navigateur.

Le tableau suivant décrit les paramètres de redirection de navigateur dans le fichier de modèle ADMX de configuration de Horizon Client. Tous les paramètres de redirection de navigateur sont des paramètres de configuration d'ordinateur. Les paramètres se trouvent dans le dossier **Configuration de VMware Horizon Client > Redirection de VMware Browser** de l'éditeur de gestion de stratégie de groupe.

Pour plus d'informations sur les paramètres de redirection de navigateur côté agent, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Tableau 3-11. Modèle de configuration de Horizon Client : paramètres de redirection de VMware Browser

Paramètre	Description
`Enable WebRTC camera and microphone access for browser redirection`	Lorsque ce paramètre est activé, les pages redirigées qui utilisent WebRTC ont accès à la caméra et au microphone du système client. Ce paramètre est activé par défaut.
`Ignore certificate errors for browser redirection`	Lorsque ce paramètre est activé, les erreurs de certificat qui se produisent dans la page redirigée sont ignorées et la navigation se poursuit. Ce paramètre est désactivé par défaut.
`Enable cache for browser redirection`	Lorsque ce paramètre est activé, l'historique de navigation, y compris les cookies, est stocké sur le système client. **Note** La désactivation de ce paramètre n'engendre pas d'effacement du cache. Si vous désactivez, puis réactivez ce paramètre, le cache est réutilisé. Ce paramètre est activé par défaut.

Paramètres de VMware Integrated Printing pour les GPO client

Vous pouvez configurer des paramètres de stratégie de groupe pour la fonctionnalité VMware Integrated Printing.

Le tableau suivant décrit les paramètres de VMware Integrated Printing dans le fichier de modèle ADMX de configuration d'Horizon Client. Le tableau montre si les paramètres incluent à la fois les paramètres Configuration ordinateur et Configuration utilisateur, ou uniquement les paramètres Configuration ordinateur. Pour les paramètres qui incluent les deux types de paramètres, le paramètre Configuration utilisateur remplace le paramètre Configuration ordinateur équivalent. Les paramètres se trouvent dans le dossier **Configuration de VMware Horizon Client > VMware Integrated Printing** de l'éditeur de gestion de stratégie de groupe.

Pour plus d'informations sur les paramètres de VMware Integrated Printing côté agent, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Tableau 3-12. Modèle de configuration d'Horizon Client : paramètres de VMware Integration Printing

Paramètre	Ordinateur	Utilisateur	Description
`Do not redirect client printer(s)`	X	X	Détermine si les imprimantes clientes sont redirigées. Lorsque ce paramètre est activé, aucune imprimante cliente n'est redirigée. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, toutes les imprimantes clientes sont redirigées. Ce paramètre n'est pas configuré par défaut.
`Allow to redirect L1 local printers to inner session`	X	X	Détermine s'il convient de rediriger les imprimantes locales L1 vers la session interne. VMware prend en charge l'exécution d'Horizon Client à l'intérieur d'un poste de travail distant. Cette configuration, communément appelée mode imbriqué, implique trois couches et deux tronçons, comme suit ■ L0 (point de terminaison) : machine physique sur laquelle Horizon Client est installé. ■ L1 (poste de travail distant du premier tronçon) : poste de travail distant sur lequel Horizon Client et Horizon Agent sont installés. ■ L2 (poste de travail publié ou application publiée du second tronçon) : application publiée ou poste de travail publié auquel le client du second tronçon se connecte. Lorsque ce paramètre est activé, les imprimantes locales L1 sont redirigées vers la session interne. Lorsque ce paramètre n'est pas configuré ou qu'il est désactivé, les imprimantes locales L1 ne sont pas redirigées vers la session interne. Ce paramètre n'est pas configuré par défaut.

Paramètres de modèle d'administration ADMX pour les variables de session de client PCoIP

Le fichier de modèle d'administration ADMX pour les variables de session de client PCoIP (`pcoip.client.admx`) contient des paramètres de stratégie liés au protocole d'affichage PCoIP. Vous pouvez configurer les valeurs par défaut de l'ordinateur qu'un administrateur peut

remplacer, ou vous pouvez configurer les paramètres d'utilisateur qu'un administrateur ne peut pas remplacer. Les paramètres qui peuvent être remplacés se trouvent dans le dossier des **Variables de session de client PCoIP > Valeurs par défaut remplaçables par l'administrateur** de l'éditeur de gestion de stratégie de groupe. Les paramètres qui ne peuvent pas être remplacés se trouvent dans le dossier **Variables de session de client PCoIP > Paramètres non remplaçables** de l'éditeur de gestion de stratégie de groupe.

Les fichiers ADMX sont disponibles dans `VMware-Horizon-Extras-Bundle-YYMM-x.x.x-yyyyyyyy.zip`, que vous pouvez télécharger sur le site de téléchargements de VMware à l'adresse https://my.vmware.com/web/vmware/downloads. Sous Informatique de bureau et d'utilisateur final, sélectionnez le téléchargement de VMware Horizon, qui comprend le bundle GPO contenant le fichier ZIP.

Tableau 3-13. Variables de session de client PCoIP

Paramètre	Description
`Configure PCoIP client image cache size policy`	Contrôle la taille du cache d'images client PCoIP. Le client utilise une mise en cache d'images pour stocker des parties de l'affichage qui ont été précédemment transmises. La mise en cache d'images réduit la quantité de données qui sont retransmises. Lorsque ce paramètre est désactivé, PCoIP utilise une taille de cache d'images client par défaut de 250 Mo. Lorsque vous activez ce paramètre, vous pouvez configurer une taille de cache d'images client comprise entre 50 Mo minimum et 300 Mo maximum. La valeur par défaut est 250 Mo. Ce paramètre est désactivé par défaut.
`Configure PCoIP event log cleanup by size in MB`	Active la configuration du nettoyage du journal des événements PCoIP par taille en Mo. Lorsque ce paramètre est configuré, il contrôle le nettoyage des fichiers journaux en fonction de la taille en Mo. Par exemple, pour une valeur de *m* différente de zéro, les fichiers journaux dont la taille est plus importante que *m* Mo sont supprimés en mode silencieux. La valeur 0 indique qu'aucun nettoyage de fichier en fonction de la taille n'est effectué. Lorsque ce paramètre est désactivé, la valeur par défaut du nettoyage du journal des événements en fonction de la taille en Mo est de 100. Ce paramètre est désactivé par défaut.
`Configure PCoIP event log cleanup by time in days`	Active la configuration du nettoyage du journal des événements PCoIP par durée en jours. Lorsque ce paramètre est configuré, il contrôle le nettoyage des fichiers journaux en fonction de la durée en jours. Par exemple, pour une valeur de *n* différente de zéro, les fichiers journaux antérieurs à *n* jours sont supprimés en mode silencieux. La valeur 0 indique qu'aucun nettoyage de fichier en fonction de la durée n'est effectué. Lorsque cette stratégie est désactivée, la valeur par défaut du nettoyage du journal des événements en fonction de la durée en jours est de 7. Ce paramètre est désactivé par défaut. Le nettoyage du fichier journal est effectué une fois au démarrage de la session. Toute modification apportée au paramètre n'est appliquée qu'à l'ouverture de la prochaine session.
`Configure PCoIP event log verbosity`	Définit le niveau de détails du journal des événements PCoIP. Les valeurs sont comprises entre 0 (le moins de détails) et 3 (le plus de détails). Lorsque ce paramètre est activé, vous pouvez définir le niveau de détail entre 0 et 3. Lorsque le paramètre est désactivé, le niveau de détail du journal des événements par défaut est de 2. Ce paramètre est désactivé par défaut. Lorsque ce paramètre est modifié lors d'une session PCoIP active, le nouveau paramètre prend effet immédiatement.

Tableau 3-13. Variables de session de client PCoIP (suite)

Paramètre	Description
`Configure PCoIP session encryption algorithms`	Contrôle les algorithmes de cryptage annoncés par le point de terminaison PCoIP lors de la négociation de session. Sélectionner l'une des cases désactive l'algorithme de cryptage associé. Vous devez activer au moins un algorithme. Ce paramètre s'applique à la fois à l'agent et au client. Les points de terminaison négocient l'algorithme de cryptage de session réel qui est utilisé. Si le mode approuvé FIPS140-2 est activé, la valeur **Désactiver le chiffrement AES-128-GCM** est remplacée si les chiffrements AES-128-GCM et AES-256-GCM sont désactivés. Si le paramètre `Configure SSL Connections` est désactivé, les deux algorithmes Salsa20-256round12 et AES-128-GCM sont disponibles pour la négociation par ce point de terminaison. Ce paramètre est désactivé par défaut. Les algorithmes de chiffrement pris en charge, par ordre de préférence, sont SALSA20/12-256, AES-GCM-128 et AES-GCM-256. Par défaut, tous les algorithmes de chiffrement pris en charge sont disponibles à la négociation à partir de ce point de terminaison.
`Configure PCoIP virtual channels`	Spécifie les canaux virtuels qui peuvent et ne peuvent pas fonctionner sur des sessions PCoIP. Ce paramètre détermine également s'il est nécessaire de désactiver le traitement du presse-papier sur l'hôte PCoIP. Les canaux virtuels utilisés dans des sessions PCoIP doivent apparaître dans la liste d'autorisation des canaux virtuels. Les canaux virtuels qui apparaissent dans la liste des canaux virtuels interdits ne peuvent pas être utilisés dans des sessions PCoIP. Vous pouvez spécifier un maximum de 15 canaux virtuels à utiliser dans des sessions PCoIP. Séparez les noms de canal avec le caractère de barre verticale (|). Par exemple, la chaîne d'autorisation des canaux virtuels pour autoriser les canaux virtuels mksvchan et vdp_rdpvcbridge est **`mksvchan|vdp_rdpvcbridge`**. Si un nom de canal contient le caractère de barre verticale ou de barre oblique inverse (\), insérez un caractère de barre oblique inverse avant ce caractère. Par exemple, saisissez le nom de canal awk|ward\channel comme suit : **`awk\\|ward\\channel`**. Lorsque la liste des canaux virtuels autorisés est vide, tous les canaux virtuels sont interdits. Lorsque la liste des canaux virtuels interdits est vide, tous les canaux virtuels sont autorisés. Le paramètre des canaux virtuels s'applique à la fois à l'agent et au client. Les canaux virtuels doivent être activés à la fois sur l'agent et le client pour pouvoir être utilisés. Le paramètre des canaux virtuels fournit une case séparée qui vous permet de désactiver le traitement du presse-papier à distance sur l'hôte PCoIP. Cette valeur ne s'applique qu'à l'agent. Par défaut, tous les canaux virtuels sont activés, notamment le traitement du presse-papier.
`Configure SSL cipher list`	Configure une liste de chiffrements TLS/SSL pour limiter l'utilisation des suites de chiffrement avant l'établissement d'une connexion TLS/SSL chiffrée. La liste se compose d'une ou de plusieurs chaînes de la suite de chiffrement séparées par deux points. Toutes les chaînes de suite de chiffrement sont insensibles à la casse. La valeur par défaut est ECDHE-RSA-AES256-GCM-SHA384:AES256-SHA256:AES256-SHA:ECDHE-RSA-AES128-GCM-SHA256:AES128-SHA256:AES128-SHA:@STRENGTH. Si ce paramètre est configuré, la case **Appliquer AES-256 ou des chiffrements plus forts pour la négociation des connexions SSL** dans le paramètre `Configure SSL connections to satisfy Security Tools` est ignorée. Ce paramètre doit être appliqué sur le serveur PCoIP et sur le client PCoIP.

Tableau 3-13. Variables de session de client PCoIP (suite)

Paramètre	Description
`Configure SSL connections to satisfy Security Tools`	Spécifie comment les connexions de négociation de session TLS sont établies. Pour satisfaire les outils de sécurité, tels que les scanners de ports, activez ce paramètre et procédez comme suit : 1 Stockez le certificat de l'autorité de certification ayant signé un certificat du serveur afin qu'il soit utilisé avec PCoIP dans le magasin de certificats racines approuvés. 2 Configurez l'agent afin qu'il charge des certificats uniquement à partir du magasin de certificats. Si le magasin personnel de la machine locale est utilisé, laissez le nom du magasin de certificats de l'autorité de certification avec la valeur « ROOT », sauf si un emplacement de magasin différent a été utilisé dans l'étape 1. Si ce paramètre est désactivé, la suite de chiffrement AES-128 n'est pas disponible. Le point de terminaison utilise alors les certificats de l'autorité de certification du magasin MY du compte de la machine et les certificats de l'autorité de certification du magasin ROOT. Ce paramètre est désactivé par défaut.
`Configure SSL protocols`	Configure le protocole OpenSSL pour restreindre l'utilisation de certains protocoles avant l'établissement d'une connexion TLS chiffrée. La liste de protocoles est composée d'une ou de plusieurs chaînes de protocole OpenSSL séparées par des caractères deux-points. Toutes les chaînes de chiffrement sont insensibles à la casse. La valeur par défaut est : `TLS1.1:TLS1.2`. Cela signifie que TLS v1.1 et TLS v1.2 sont activés et que SSL v2.0, SSL v3.0 et TLS v1.0 sont désactivés. Si ce paramètre est défini dans le client et l'agent, la règle de négociation du protocole OpenSSL est suivie.
`Configure the Client PCoIP UDP port`	Spécifie le port client UDP utilisé par les clients PCoIP logiciels. La valeur du port UDP spécifie le port UDP de base à utiliser. Si le port de base n'est pas disponible, la valeur de plage de ports UDP détermine le nombre de ports supplémentaires à essayer. La plage s'étend du port de base à la somme du port de base et de la plage du port. Par exemple, si le port de base est 50002 et que la plage du port est 64, la plage s'étend de 50002 à 50066. Ce paramètre ne s'applique qu'au client. Par défaut, le port de base est 50002 et la plage du port est 64.

Tableau 3-13. Variables de session de client PCoIP (suite)

Paramètre	Description
`Configure the maximum PCoIP session bandwidth`	Spécifie la bande passante maximale, en kilobits par seconde, dans une session PCoIP. La bande passante inclut la création d'images, le son, le canal virtuel, USB et le trafic PCoIP de contrôle. Définissez cette valeur sur la capacité globale du lien auquel votre point de terminaison est connecté, en tenant compte du nombre de sessions PCoIP simultanées prévues. Par exemple, avec une configuration VDI à un seul utilisateur (une session PCoIP unique) qui se connecte au moyen d'une connexion Internet 4 Mbits/s, définissez cette valeur sur 4 Mbit, ou 10 % de moins que cette valeur pour prévoir un autre trafic réseau. Lorsque vous prévoyez que plusieurs sessions PCoIP simultanées partageront un lien, comprenant plusieurs utilisateurs VDI ou une configuration RDS, vous pouvez régler ce paramètre en conséquence. Cependant, la diminution de cette valeur limitera la bande passante maximale de chaque session active. La définition de cette valeur empêche l'agent de transmettre un débit supérieur à la capacité de lien, ce qui pourrait entraîner une perte de paquets excessive et une mauvaise expérience utilisateur. Cette valeur est symétrique. Elle force le client et l'agent à utiliser la plus faible des deux valeurs qui sont définies côté client et agent. Par exemple, la définition d'une bande passante maximale de 4 Mbit/s force l'agent à transmettre à un débit plus faible, même si le paramètre est configuré sur le client. Lorsque ce paramètre est désactivé sur un point de terminaison, le point de terminaison n'impose aucune contrainte de bande passante. Lorsque ce paramètre est activé, il est utilisé comme la contrainte de bande passante maximale du point de terminaison en kilobits par seconde. La valeur par défaut est de 900 000 kilobits par seconde. Ce paramètre s'applique à la fois à l'agent et au client. Si les deux points de terminaison ont des paramètres différents, la valeur la plus faible est utilisée.
`Configure the PCoIP session bandwidth floor`	Spécifie une limite inférieure, en kilobits par seconde, pour la bande passante réservée par la session PCoIP. Ce paramètre configure le taux de transmission de bande passante minimum attendu pour le point de terminaison. Lorsque vous utilisez ce paramètre pour réserver de la bande passante pour un point de terminaison, l'utilisateur n'a pas à attendre que la bande passante soit disponible, ce qui améliore la réactivité de la session. Assurez-vous que vous ne sursouscrivez pas la bande passante totale réservée pour tous les points de terminaison. Assurez-vous que la somme des valeurs plancher de la bande passante pour toutes les connexions dans votre configuration ne dépasse pas la capacité du réseau. La valeur par défaut est 0, ce qui signifie qu'aucune bande passante minimale n'est réservée. Lorsque ce paramètre est désactivé, aucune bande passante minimale n'est réservée. Ce paramètre est désactivé par défaut. Ce paramètre s'applique à l'agent et au client, mais le paramètre n'affecte que le point de terminaison sur lequel il est configuré. Lorsque ce paramètre est modifié lors d'une session PCoIP active, la modification prend effet immédiatement.

Tableau 3-13. Variables de session de client PCoIP (suite)

Paramètre	Description
`Configure the PCoIP session MTU`	Spécifie la taille de l'unité de transmission maximale (MTU) pour les paquets UDP d'une session PCoIP. La taille de la MTU inclut les en-têtes de paquet IP et UDP. Le protocole TCP utilise le mécanisme de découverte MTU standard pour définir la MTU et ce paramètre ne l'affecte pas. La taille de la MTU maximale est de 1 500 octets. La taille de la MTU minimale est de 500 octets. La valeur par défaut est de 1 300 octets. En général, vous n'avez pas à modifier la taille de la MTU. Modifiez cette valeur si vous avez une configuration de réseau inhabituelle qui provoque une fragmentation de paquets PCoIP. Ce paramètre s'applique à la fois à l'agent et au client. Si les deux points de terminaison ont des paramètres de taille de MTU différents, la valeur la plus faible est utilisée. Si ce paramètre est désactivé ou qu'il n'est pas configuré, le client utilise la valeur par défaut dans la négociation avec l'agent.
`Configure the PCoIP transport header`	Configure l'en-tête de transport PCoIP et définit la priorité de la session de transport. L'en-tête de transport PCoIP est un en-tête 32 bits qui est ajouté à tous les paquets UDP PCoIP (uniquement si l'en-tête de transport est activé et pris en charge des deux côtés). L'en-tête de transport PCoIP permet aux périphériques réseau de prendre de meilleures décisions concernant la hiérarchisation/qualité de service lors du traitement de la surcharge du réseau. L'en-tête de transport est activé par défaut. La priorité de session de transport détermine la priorité de session PCoIP signalée dans l'en-tête de transport PCoIP. Les périphériques réseau prennent de meilleures décisions concernant la hiérarchisation/qualité de service en fonction de la priorité de session de transport spécifiée. Lorsque le paramètre `Configure the PCoIP transport header` est activé, les priorités de session de transport suivantes sont disponibles : ■ **Haute** ■ **Moyenne** (valeur par défaut) ■ **Basse** ■ **Non définie** L'agent PCoIP et le client négocient la valeur de priorité de session de transport. Si l'agent PCoIP spécifie une valeur de priorité de session de transport, la session utilise la priorité de session spécifiée par l'agent. Si seul le client a spécifié une priorité de session de transport, la session utilise la priorité de session spécifiée par le client. Si ni l'agent ni le client n'a spécifié une priorité de session de transport, ou si **Priorité non définie** est spécifié, la session utilise la valeur par défaut, la priorité **Moyenne**.
`Enable/disable audio in the PCoIP session`	Détermine si le son est activé dans des sessions PCoIP. Le son doit être activé sur les deux points de terminaison. Lorsque ce paramètre est activé, le son PCoIP est autorisé. Lorsqu'il est désactivé, le son PCoIP est désactivé. Le son est activé par défaut.

Exécution d'Horizon Client depuis la ligne de commande

Vous pouvez exécuter Horizon Client à partir de la ligne de commande ou via des scripts. Vous pouvez exécuter Horizon Client à partir de la ligne de commande si vous mettez en place une application kiosque qui accorde l'accès des utilisateurs finaux aux applications de poste de travail distant.

Pour exécuter Horizon Client à partir de la ligne de commande, vous utilisez la commande `vmware-view.exe`. La commande `vmware-view.exe` inclut des options que vous pouvez spécifier pour modifier le comportement d'Horizon Client.

Utilisation des commandes Horizon Client

La syntaxe de la commande `vmware-view` contrôle le fonctionnement d'Horizon Client.

Utilisez la forme suivante de la commande `vmware-view` à partir d'une invite de commande Windows.

```
vmware-view [command_line_option [argument]] ...
```

Le chemin d'accès par défaut au fichier exécutable de la commande `vmware-view` varie en fonction du système client. Vous pouvez ajouter ce chemin d'accès à la variable d'environnement *PATH* sur le système client.

- Systèmes 32 bits : `C:\Program Files\VMware\VMware Horizon View Client\`
- Systèmes 64 bits : `C:\Program Files (x86)\VMware\VMware Horizon View Client\`

Le tableau suivant présente les options de ligne de commande que vous pouvez utiliser avec la commande `vmware-view`.

Tableau 3-14. Options de ligne de commande d'Horizon Client

Option	Description
`/?`	Affiche la liste d'options de commande.
`-appName` *application_name*	Spécifie le nom de l'application publiée tel qu'il apparaît dans la fenêtre de sélection des postes de travail et applications. Il s'agit du nom d'affichage spécifié pour le pool d'applications dans l'assistant de création de pool.
`-appProtocol` *protocol*	Spécifie le protocole d'affichage de l'application publiée à utiliser, si disponible. Les protocoles valides sont les suivants : ■ **`VMware Blast`** ■ **`PCoIP`**
argument `-appSessionReconnectionBehavior`	Spécifie le paramètre de comportement de reconnexion des applications publiées. Les arguments valides sont les suivants : **`always`** Met en œuvre le paramètre **Se reconnecter automatiquement pour ouvrir des applications**. **`never`** Met en œuvre le paramètre **Ne pas demander la reconnexion et ne pas se reconnecter automatiquement**. **`ask`** Met en œuvre le paramètre **Demander la reconnexion pour ouvrir des applications**. Lorsque vous utilisez cette option, les paramètres de reconnexion d'applications publiées sont désactivés dans Horizon Client.

Tableau 3-14. Options de ligne de commande d'Horizon Client (suite)

Option	Description
argument `-args`	Spécifie les arguments de ligne de commande à ajouter au démarrage d'une application publiée. Par exemple : `vmware-view.exe --serverURL 10.10.10.10 --appName "My Notepad++" --args "\"my new.txt\""`
`-connectUSBOnStartup`	Lorsque cette est définie sur `true`, tous les périphériques USB actuellement connectés à l'hôte sont redirigés vers le poste de travail distant ou l'application publiée. Cette option est implicitement définie si vous spécifiez l'option `-unattended` pour un poste de travail distant. L'option par défaut est `false`.
`-connectUSBOnInsert`	Lorsque défini sur `true`, connecte un périphérique USB au poste de travail distant ou à l'application publiée au premier plan lorsque vous branchez le périphérique. Cette option est implicitement définie si vous spécifiez l'option `-unattended` pour un poste de travail distant. L'option par défaut est `false`.
`-desktopLayout` *window_size*	Spécifie comment afficher la fenêtre du poste de travail distant. Les valeurs de taille de fenêtre valides sont les suivantes : **`fullscreen`** Affichage en plein écran. **`multimonitor`** Affichage sur plusieurs moniteurs. **`windowLarge`** Fenêtre de grande taille. **`windowSmall`** Fenêtre de petite taille. **`length X width`** Taille personnalisée, par exemple, 800 × 600.
`-desktopName` *desktop_name*	Spécifie le nom du poste de travail distant tel qu'il apparaît dans la fenêtre de sélection des postes de travail et applications. Il s'agit du nom d'affichage spécifié pour le pool dans l'assistant de création de pool. **Important** Ne spécifiez pas cette option pour les clients en mode kiosque. Cette option n'a aucun effet lorsque le poste de travail distant s'exécute en mode kiosque. Pour le mode kiosque, la connexion est établie au premier poste de travail distant dans la liste des postes de travail distants octroyés.
`-desktopProtocol` *protocol*	Spécifie le protocole d'affichage à utiliser tel qu'il il apparaît dans la fenêtre de sélection des postes de travail et applications. Les protocoles d'affichage valides sont les suivants : ■ **`Blast`** ■ **`PCoIP`** ■ **`RDP`**
`-domainName` *domain_name*	Spécifie le domaine NETBIOS que l'utilisateur final utilise pour ouvrir une session d'Horizon Client. Utilisez par exemple `monentreprise` plutôt que `monentreprise.com`.
`-file` *file_path*	Spécifie le chemin d'un fichier de configuration qui contient des options et des arguments de commande supplémentaires. Reportez-vous à la section Consulter le fichier de configuration Horizon Client.

Tableau 3-14. Options de ligne de commande d'Horizon Client (suite)

Option	Description
`-h`	Affiche les options de l'aide.
`-hideClientAfterLaunchSession`	Lorsque cette option est définie sur `true`, la fenêtre de sélection des applications et des postes de travail et le menu **Afficher VMware Horizon Client** sont masqués après le démarrage d'une session à distance. Lorsque cette option est définie sur `false`, la fenêtre de sélection des applications et des postes de travail et le menu **Afficher VMware Horizon Client** sont affichés après le démarrage d'une session à distance. L'option par défaut est `true`.

`-installShortcutsThenQuit`	Utilisez cette option pour installer des raccourcis de poste de travail et d'application qui sont configurés sur le serveur. Lorsque vous utilisez cette option avec des informations d'authentification de serveur suffisantes, Horizon Client se connecte au serveur en silence, installe les raccourcis, puis se ferme. Si l'authentification du serveur échoue, Horizon Client se ferme en silence.
	Pour installer automatiquement des raccourcis sur le système client, créez un script qui s'exécute lors du démarrage du système client. Par exemple :
	`vmware-view.exe -serverURL serverurl -userName user -domainName domain -password password -installShortcutsThenQuit`
	`vmware-view.exe -serverURL serverurl -loginAsCurrentUser true -installShortcutsThenQuit`
	Pour plus d'informations sur les raccourcis créés par le serveur, reportez-vous à la section Utilisation des raccourcis créés par le serveur.

`-languageId` *Locale_ID*	Assure la localisation de différentes langues dans Horizon Client. Si une bibliothèque de ressources est disponible, spécifiez l'ID de paramètre local (LCID) à utiliser. Pour l'anglais US, saisissez la valeur 0x409.
`-launchMinimized`	Démarre Horizon Client en mode réduit. Si vous indiquez l'option `-appName` ou `-desktopName`, Horizon Client reste réduit jusqu'au démarrage de l'application publiée ou du poste de travail distant spécifié. Vous ne pouvez pas utiliser cette option avec l'option `-unattended` ou `-nonInteractive`.

`-listMonitors`	Répertorie les valeurs d'index et les informations de disposition de l'affichage des moniteurs connectés. Par exemple :
	`1: (0, 0, 1920, 1200)`
	`2: (1920, 0, 3840, 1200)`
	`3: (-900, -410, 0, 1190)`
	Vous pouvez utiliser ces valeurs d'index dans l'option `-monitors`.

`-logInAsCurrentUser`	Lorsque cette valeur est définie sur `true`, les informations d'identification que l'utilisateur final fournit lors de l'ouverture de session sur le système client pour se connecter au serveur, puis au poste de travail distant, sont utilisées. L'option par défaut est `false`.

Tableau 3-14. Options de ligne de commande d'Horizon Client (suite)

Option	Description
`-monitors "n[,n,n,n]"`	Spécifie les moniteurs à utiliser dans une configuration à plusieurs moniteurs, où *n* est la valeur d'index d'un moniteur. Vous pouvez utiliser l'option `-listMonitors` pour déterminer les valeurs d'index des moniteurs connectés. Vous pouvez spécifier jusqu'à quatre valeurs d'index, séparées par des virgules. Par exemple : `-monitors "1,2"` Cette option n'a pas d'effet tant que `-desktopLayout` n'est pas défini sur `multimonitor`.
`-nonInteractive`	Supprime des zones de messages d'erreur lors du démarrage d'Horizon Client à partir d'un script. Cette option est implicitement définie si vous spécifiez l'option `-unattended`. **Note** Si vous vous connectez à un serveur en mode non interactif, vous n'êtes pas invité à installer les raccourcis du menu **Démarrer** (le cas échéant) et des raccourcis sont installés par défaut.
`-noVMwareAddins`	Empêche le chargement de canaux virtuels spécifiques de VMware tels que l'impression virtuelle.
`-password` *password*	Spécifie le mot de passe que l'utilisateur final utilise pour ouvrir une session d'Horizon Client. La console de commande ou tout outil de script traite le mot de passe en texte brut. Si vous générez le mot de passe automatiquement, il est inutile de spécifier cette option pour les clients en mode kiosque. Pour améliorer la sécurité, ne spécifiez pas cette option. Les utilisateurs peuvent entrer le mot de passe de façon interactive.
`-printEnvironmentInfo`	Affiche l'adresse IP, l'adresse MAC et le nom de machine du périphérique client.
`-serverURL` *connection_server*	Spécifie l'URL, l'adresse IP ou le nom de domaine complet du serveur.
`-shutdown`	Arrête tous les postes de travail distants et applications publiées et les composants d'interface utilisateur pertinents.
`-singleAutoConnect`	Si l'utilisateur n'est autorisé à se connecter qu'à un seul poste de travail distant ou à une seule application publiée, la connexion à ce poste de travail distant ou à cette application publiée est établie une fois que l'utilisateur s'est authentifié auprès du serveur. Ce paramètre permet à l'utilisateur de ne pas sélectionner un poste de travail distant ou une application publiée dans une liste contenant un seul élément.
`-smartCardPIN` *PIN*	Spécifie le code PIN lorsqu'un utilisateur final insère une carte à puce pour ouvrir une session.
`-usernameHint` *user_name*	Spécifie le nom de compte à utiliser comme aide-mémoire du nom d'utilisateur.

Tableau 3-14. Options de ligne de commande d'Horizon Client (suite)

Option	Description
`-standalone`	Démarre une deuxième instance d'Horizon Client qui peut se connecter au même serveur ou à un autre serveur. Cette option est prise en charge pour la compatibilité en amont. Il n'est pas nécessaire de spécifier le paramètre `-standalone`, car il s'agit du comportement par défaut du client. Pour plusieurs connexions de poste de travail distant au même serveur ou à un autre serveur, l'utilisation du tunnel sécurisé est prise en charge. **Note** La seconde connexion de poste de travail peut ne pas avoir accès au matériel local, tel que les périphériques USB, les cartes à puce, les imprimantes et les écrans multiples.
`-supportText` *file_name*	Spécifie le chemin d'accès complet d'un fichier texte. Le contenu du fichier est affiché dans la boîte de dialogue Informations de support.
`-unattended`	Démarre Horizon Client dans un mode non interactif approprié aux clients en mode Kiosque. Vous devez également spécifier les informations suivantes : ■ Le nom de compte du client, si vous n'avez pas généré le nom de compte à partir de l'adresse MAC du périphérique client. Le nom doit commencer par la chaîne de caractères « custom- » ou par un autre préfixe que vous avez configuré dans ADAM. ■ Le mot de passe du client, si vous n'avez pas généré un mot de passe automatiquement lorsque vous avez configuré le compte pour le client. L'option `-unattended` définit implicitement les options `-nonInteractive`, `-connectUSBOnStartup`, `-connectUSBOnInsert` et `-desktopLayout multimonitor`.
`-unauthenticatedAccessAccount`	Spécifie un compte d'utilisateur Accès non authentifié à utiliser pour se connecter de manière anonyme au serveur lorsque l'accès non authentifié est activé. Si l'accès non authentifié n'est pas activé, cette option est ignorée. Par exemple : `vmware-view.exe -serverURL view.mycompany.com -unauthenticatedAccessEnabled true -unauthenticatedAccessAccount anonymous1`
`-unauthenticatedAccessEnabled`	Lorsque cette valeur est définie sur `true`, l'accès non authentifié est autorisé. Si l'accès non authentifié n'est pas disponible, le client peut revenir à une autre méthode d'authentification. Le paramètre **Se connecter de manière anonyme à l'aide de l'accès non authentifié** est affiché, désactivé et sélectionné dans Horizon Client. Lorsque cette valeur est définie sur `false`, vous devez saisir vos informations d'identification pour vous connecter à vos applications et y accéder. Le paramètre **Se connecter de manière anonyme à l'aide de l'accès non authentifié** est masqué et désélectionné dans Horizon Client. Si vous ne spécifiez pas cette option, vous pouvez activer l'accès non authentifié dans Horizon Client. Le paramètre **Se connecter de manière anonyme à l'aide de l'accès non authentifié** est affiché, activé et désélectionné.

Tableau 3-14. Options de ligne de commande d'Horizon Client (suite)

Option	Description

`-useExisting`	Cette option vous permet de lancer plusieurs applications publiées et postes de travail distants à partir d'une seule session Horizon Client.
	Lorsque vous spécifiez cette option, Horizon Client détermine si une session avec les mêmes nom d'utilisateur, domaine et URL de serveur existe déjà et, si c'est le cas, réutilise cette session au lieu d'en créer une.
	Par exemple, dans la commande suivante, user-1 démarre l'application Calculatrice et une session est créée.
	`vmware-view.exe -userName user-1 -password secret -domainName domain -appName Calculator -serverURL view.mycompany.com -useExisting`
	Dans la commande suivante, user1 démarre l'application Paint avec les mêmes nom d'utilisateur, domaine et URL de serveur, et la même session est utilisée.
	`vmware-view.exe -userName user-1 -password secret -domainName domain -appName Paint -serverURL view.mycompany.com -useExisting`

`-userName` *user_name*	Spécifie le nom de compte que l'utilisateur final utilise pour ouvrir une session d'Horizon Client. Si vous générez le nom du compte de l'adresse MAC du périphérique client, vous n'avez pas besoin spécifier cette option pour les clients en mode kiosque.

Vous pouvez spécifier toutes les options par des stratégies de groupe Active Directory, à l'exception de `-file`, `-languageId`, `-printEnvironmentInfo`, `-smartCardPIN` et `-unattended`.

Note Les paramètres de stratégie de groupe prévalent sur ceux spécifiés dans la ligne de commande.

Consulter le fichier de configuration Horizon Client

Vous pouvez consulter les options de ligne de commande pour Horizon Client dans un fichier de configuration.

Vous pouvez spécifier le chemin du fichier de configuration comme argument de l'option `-file` *file_path* de la commande `vmware-view`. Le fichier doit être un fichier texte Unicode (UTF-16) ou ASCII.

Exemple : Exemple de fichier de configuration pour une application non interactive

L'exemple suivant montre le contenu d'un fichier de configuration pour une application non interactive.

```
-serverURL https://view.yourcompany.com
-userName autouser
-password auto123
-domainName companydomain
```

```
-desktopName autodesktop
-nonInteractive
```

Exemple : Exemple de fichier de configuration pour un client en mode kiosque

L'exemple suivant montre un client en mode kiosque dont le nom de compte est basé sur son adresse MAC. Le client a un mot de passe généré automatiquement.

```
-serverURL 145.124.24.100
-unattended
```

Utilisation du Registre Windows pour configurer Horizon Client

Vous pouvez définir des paramètres par défaut pour Horizon Client dans le registre Windows plutôt que de les spécifier sur la ligne de commande. Les paramètres de stratégie de groupe prévalent sur les paramètres du registre Windows, et les paramètres du registre Windows prévalent sur la ligne de commande.

Note Dans une future version d'Horizon Client, les paramètres du registre Windows peuvent ne pas être pris en charge et les paramètres de stratégie de groupe doivent être utilisés.

Le tableau suivant répertorie les paramètres du registre pour la connexion à Horizon Client. Ces paramètres se trouvent sous `HKEY_CURRENT_USER\Software\VMware, Inc.\VMware VDM\Client\` dans le registre. Cet emplacement est spécifique à un utilisateur particulier. Les paramètres `HKEY_LOCAL_MACHINE`, qui sont décrits dans le tableau suivant, sont des paramètres au niveau de l'ordinateur et relatifs à tous les utilisateurs locaux et à tous les utilisateurs du domaine qui sont autorisés à se connecter à l'ordinateur dans un environnement de domaine Windows.

Tableau 3-15. Paramètres de registre Horizon Client pour les informations d'identification

Paramètre de registre	Description
`Mot de passe`	Mot de passe par défaut.
`Nom d'utilisateur`	Nom d'utilisateur par défaut.

Le tableau suivant répertorie les paramètres du registre pour Horizon Client qui n'incluent pas les informations d'identification. L'emplacement de ces paramètres dépend du type de système utilisé :

- Pour Windows 32 bits : `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\`
- Pour Windows 64 bits : `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\`

Tableau 3-16. Paramètres de registre d'Horizon Client

Paramètre de registre	Description
`DomainName`	Nom de domaine NETBIOS par défaut. Utilisez par exemple `monentreprise` plutôt que `monentreprise.com`.
`EnableShade`	Détermine si la barre de menus (ombre) en haut de la fenêtre d'Horizon Client doit être activée. Elle l'est par défaut sauf pour les clients en mode kiosque. La valeur **`false`** désactive la barre de menus. **Note** Ce paramètre s'applique uniquement lorsque la disposition d'affichage est définie sur **Tous les moniteurs** ou **Plein écran**.
`ServerURL`	URL, adresse IP ou nom de domaine complet de l'instance du Serveur de connexion par défaut.
`EnableSoftKeypad`	Si cette valeur est définie sur **`true`** et qu'une fenêtre Horizon Client est activée, les événements du clavier physique, du clavier à l'écran, de la souris et du pavé d'écriture sont envoyés vers le poste de travail distant ou l'application publiée, même si la souris ou le clavier à l'écran se trouve à l'extérieur de la fenêtre Horizon Client. La valeur par défaut est **`false`**.

Le tableau suivant indique les paramètres de sécurité que vous pouvez ajouter. L'emplacement de ces paramètres dépend du type de système utilisé :

- Pour Windows 32 bits : `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security`
- Pour Windows 64 bits : `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security`

Tableau 3-17. Paramètres de sécurité

Paramètre de registre	Description et valeurs valides
`CertCheckMode`	Mode de vérification des certificats. Les valeurs valides sont les suivantes : ■ **0** implémente `Do not verify server identity certificates.` ■ **1** implémente `Warn before connecting to untrusted servers.` ■ **2** implémente `Never connect to untrusted servers.`
`SSLCipherList`	Configure la liste de chiffrements afin de limiter l'utilisation de certains protocoles et algorithmes de chiffrement avant l'établissement d'une connexion TLS chiffrée. La liste de chiffrements est composée d'une ou de plusieurs chaînes de chiffrement séparées par deux points. Toutes les chaînes de chiffrement sont sensibles à la casse. La valeur par défaut est **TLSv1.1:TLSv1.2:!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES**. La valeur par défaut signifie que TLS v1.1 et TLS v1.2 sont activés et que SSL v.2.0, SSL v3.0 et TLS v1.0 sont désactivés. SSL v2.0, SSL v3.0 et TLS v1.0 ne sont plus les protocoles approuvés et sont définitivement désactivés. Les suites de chiffrement utilisent la spécification AES 128 ou 256 bits, suppriment les algorithmes DH anonymes, et trient la liste de chiffrements actuels par longueur de clé de chiffrement. Pour des informations de référence sur la configuration, reportez-vous à la page http://www.openssl.org/docs/apps/ciphers.html .

Gestion des connexions aux postes de travail distants et applications publiées

4

Les utilisateurs finaux peuvent utiliser Horizon Client pour se connecter à un serveur, pour ouvrir ou fermer une session sur les postes de travail distants et pour utiliser des applications publiées. À des fins de dépannage, les utilisateurs finaux peuvent également redémarrer et réinitialiser les postes de travail distants et les applications publiées.

En fonction de la façon dont vous configurez les stratégies, les utilisateurs finaux peuvent être en mesure d'exécuter plusieurs opérations sur leurs postes de travail distants et applications publiées.

Ce chapitre contient les rubriques suivantes :

- Se connecter à un poste de travail distant ou à une application publiée
- Utiliser l'accès non authentifié pour se connecter à des applications publiées
- Partager des informations d'emplacement
- Masquer la fenêtre VMware Horizon Client
- Reconnexion à un poste de travail distant ou une application publiée
- Créer un raccourci sur le bureau du Client Windows ou dans le menu Démarrer
- Utilisation des raccourcis créés par le serveur
- Configurer la fonction de connexion automatique pour un poste de travail distant
- Fermer une session ou se déconnecter
- Déconnexion d'un serveur

Se connecter à un poste de travail distant ou à une application publiée

Pour vous connecter à un poste de travail distant ou une application publiée, vous devez fournir le nom d'un serveur et entrer les informations d'identification de votre compte d'utilisateur.

Avant de laisser vos utilisateurs finaux accéder à leurs applications publiées et postes de travail distants, vérifiez que vous pouvez vous connecter à une application publiée ou à un poste de travail distant à partir d'un périphérique client. Vous devrez peut-être spécifier un serveur et fournir des informations d'identification pour votre compte d'utilisateur.

Conditions préalables

- Procurez-vous les informations d'identification de connexion, telles que le nom d'utilisateur et le mot de passe, le nom d'utilisateur et le code secret RSA SecurID, les informations d'identification pour l'authentification RADIUS ou le numéro d'identification personnel (PIN) de carte à puce.
- Obtenez le nom de domaine NETBIOS pour ouvrir une session. Utilisez par exemple `monentreprise` plutôt que `monentreprise.com`.
- Effectuez les tâches administratives décrites dans Préparation du Serveur de connexion pour Horizon Client.
- Si vous vous trouvez à l'extérieur du réseau de l'entreprise et que vous devez utiliser une connexion VPN pour accéder à des postes de travail distants ou à des applications publiées, vérifiez que le périphérique client est configuré pour utiliser une connexion VPN et activez la connexion.
- Vérifiez que vous disposez du nom de domaine complet (FQDN) du serveur qui fournit l'accès au poste de travail distant ou à l'application publiée. Les traits de soulignement (_) ne sont pas pris en charge dans les noms de serveur. Si le port n'est pas le port 443, vous avez également besoin du numéro de port.
- Si vous prévoyez d'utiliser le protocole d'affichage RDP pour vous connecter à un poste de travail distant, vérifiez que le paramètre de stratégie de groupe AllowDirectRDP de l'agent est activé. Pour plus d'informations, consultez le document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.
- Configurez le mode de vérification des certificats pour le certificat présenté par le serveur. Pour savoir quel mode utiliser, reportez-vous à la section Définition du mode de vérification des certificats dans Horizon Client.

Procédure

1. Si une connexion VPN est requise, activez le VPN.
2. Démarrez Horizon Client.
3. (Facultatif) Pour vous connecter en tant qu'utilisateur de domaine Windows actuellement connecté, cliquez sur le bouton **Options** dans le coin supérieur droit de la barre de menus et sélectionnez **Se connecter en tant qu'utilisateur actuel**.

   Ce paramètre est disponible uniquement si la fonctionnalité **Se connecter en tant qu'utilisateur actuel** est installée sur le système client.

4 Connectez-vous à un serveur.

Option	Action
Se connecter à un nouveau serveur	Double-cliquez sur le bouton **+ Ajouter un serveur** ou cliquez sur **Nouveau serveur** dans la barre de menus, entrez le nom d'un serveur et cliquez sur **Se connecter**.
Se connecter à un serveur existant	Double-cliquez sur l'icône du serveur, ou cliquez avec le bouton droit sur l'icône du serveur, puis sélectionnez **Se connecter**.

Les connexions entre Horizon Client et le serveur utilisent toujours TLS. Le port par défaut pour les connexions TLS est 443. Si le serveur n'est pas configuré pour utiliser le port par défaut, utilisez le format *nomdeserveur :port*, par exemple, **`view.company.com:1443`**.

Vous pouvez voir un message que vous devez confirmer avant que la boîte de dialogue de connexion apparaisse.

5 Si un message demande les informations d'identification RSA SecurID ou les informations d'identification pour l'authentification RADIUS, entrez-les, puis cliquez sur **Continuer**.

6 Saisissez les informations d'identification d'un utilisateur autorisé à utiliser au moins un pool de postes de travail distants ou d'applications publiées, sélectionnez le domaine et cliquez sur **Ouvrir une session**.

Si vous entrez le nom d'utilisateur en tant que **`nom d'utilisateur@domaine`**, Horizon Client le traite comme un nom d'utilisateur principal (UPN) et le menu déroulant **Domaine** est désactivé.

Si le menu déroulant **Domaine** est masqué, vous devez entrer le nom d'utilisateur sous la forme ***`nomutilisateur`*`@`*`domaine`** ou ***`domaine`*`\`*`nomutilisateur`**.

7 Si Horizon Client vous invite à installer les applications publiées ou les postes de travail distants dans le menu **Démarrer** de Windows, cliquez sur **Oui** ou **non**.

Cette invite peut s'afficher la première fois que vous vous connectez à un serveur sur lequel les raccourcis ont été configurés pour les applications publiées ou les postes de travail distants. Si vous cliquez sur **Oui**, les raccourcis du menu **Démarrer** sont installés sur le système client pour ces applications publiées ou les postes de travail distants, si vous êtes autorisé à les utiliser. Si vous cliquez sur **Non**, les raccourcis du menu **Démarrer** ne sont pas installés.

Un administrateur Horizon peut configurer le paramètre de stratégie de groupe **Installer automatiquement des raccourcis s'ils sont configurés sur Horizon Server** pour inviter les utilisateurs finaux à installer des raccourcis (la valeur par défaut), à installer automatiquement les raccourcis ou à ne jamais installer les raccourcis.

8 (Facultatif) Pour configurer les paramètres d'affichage d'un poste de travail distant, cliquez avec le bouton droit sur l'icône du poste de travail distant, puis sélectionnez **Paramètres**.

Option	Action
Sélectionner un protocole d'affichage	Si l'administrateur Horizon l'a autorisé, utilisez le menu déroulant **Connecter via** pour sélectionner le protocole d'affichage.
Sélectionner une disposition d'affichage	Utilisez le menu déroulant **Affichage** pour sélectionner une taille de fenêtre ou pour utiliser plusieurs écrans.

9 Pour vous connecter à un poste de travail distant ou à une application publiée, double-cliquez sur l'icône du poste de travail distant ou de l'application publiée dans la fenêtre de sélection des postes de travail et applications.

Si vous vous connectez à un poste de travail publié et si celui-ci est déjà configuré pour utiliser un autre protocole d'affichage, vous ne pouvez pas vous connecter immédiatement. Horizon Client vous invite à utiliser le protocole défini ou à fermer votre session pour que Horizon Client puisse se connecter avec un protocole d'affichage différent.

Résultats

Une fois que vous êtes connecté, le poste de travail distant ou l'application publiée s'ouvre.

Si vous êtes autorisé à vous connecter à plusieurs postes de travail distants ou applications publiées sur le serveur, la fenêtre de sélection des postes de travail et applications reste ouverte afin que vous puissiez vous connecter à plusieurs postes de travail distants et applications publiées.

Si la fonctionnalité de redirection du lecteur client est activée, la boîte de dialogue Partage s'affiche et vous pouvez autoriser ou refuser l'accès aux fichiers sur le système de fichiers local. Pour plus d'informations, reportez-vous à la section Partager des lecteurs et des dossiers locaux.

La première fois que vous vous connectez à un serveur, Horizon Client enregistre un raccourci vers le serveur dans la fenêtre d'accueil d'Horizon Client. Vous pouvez double-cliquer sur ce raccourci du serveur la prochaine fois que vous devez vous y connecter.

Si l'authentification sur le serveur échoue ou si le client ne peut pas se connecter à une application publiée ou à un poste de travail distant, effectuez les tâches suivantes :

- Vérifiez que le certificat du serveur fonctionne correctement. Si tel n'est pas le cas, dans Horizon Console, l'agent sur des postes de travail ne sera peut-être pas accessible. Ces symptômes indiquent qu'il existe d'autres problèmes de connexion causés par des problèmes de certificat.
- Vérifiez que les balises définies sur l'instance du Serveur de connexion autorisent les connexions depuis cet utilisateur. Reportez-vous au document *Administration d'Horizon*.
- Vérifiez que l'utilisateur est autorisé à accéder au poste de travail distant ou à l'application publiée. Reportez-vous au document *Configuration des postes de travail virtuels dans Horizon* ou *Configuration d'applications et de postes de travail publiés dans Horizon*.

- Si vous utilisez le protocole d'affichage RDP pour vous connecter à un poste de travail distant, vérifiez que le système d'exploitation du poste de travail distant autorise les connexions à des postes de travail distants.

Étape suivante

Configurez les paramètres de démarrage. Si vous ne voulez pas que les utilisateurs finaux fournissent le nom d'hôte du serveur ou si vous souhaitez configurer d'autres paramètres de démarrage, utilisez une option de ligne de commande pour créer un raccourci de poste de travail distant. Reportez-vous à la section Exécution d'Horizon Client depuis la ligne de commande.

Utiliser l'accès non authentifié pour se connecter à des applications publiées

Si vous disposez d'un compte d'utilisateur Accès non authentifié, vous pouvez vous connecter à un serveur de manière anonyme et vous connecter à vos applications publiées.

Avant de laisser les utilisateurs finaux accéder à une application publiée avec la fonctionnalité Accès non authentifié, vérifiez que vous pouvez vous connecter à l'application publiée à partir d'un périphérique client. Vous devrez peut-être spécifier un serveur et fournir des informations d'identification pour votre compte d'utilisateur.

Par défaut, les utilisateurs sélectionnent le paramètre **Se connecter de manière anonyme à l'aide de l'accès non authentifié** du menu **Options** et sélectionnent un compte d'utilisateur pour se connecter de manière anonyme. Un administrateur Horizon peut configurer les paramètres de stratégie de groupe de manière à présélectionner le paramètre **Se connecter de manière anonyme à l'aide de l'accès non authentifié** et permettre aux utilisateurs de se connecter à l'aide d'un compte d'utilisateur Accès non authentifié spécifique.

Conditions préalables

- Effectuez les tâches administratives décrites dans Préparation du Serveur de connexion pour Horizon Client.
- Configurez des utilisateurs avec un accès non authentifié sur l'instance du Serveur de connexion. Pour plus d'informations, consultez « Fournir un accès non authentifié pour des applications publiées » dans le document *Administration d'Horizon*.
- Si vous êtes à l'extérieur du réseau d'entreprise, vérifiez que votre périphérique client est configuré pour utiliser une connexion VPN et activez cette connexion.
- Vérifiez que vous disposez du nom de domaine complet (FQDN) du serveur qui fournit l'accès à l'application publiée. Les traits de soulignement (_) ne sont pas pris en charge dans les noms de serveur. Si le port n'est pas le port 443, vous avez également besoin du numéro de port.
- Configurez le mode de vérification des certificats pour le certificat présenté par le serveur dans Horizon Client. Pour savoir quel mode utiliser, reportez-vous à la section Définition du mode de vérification des certificats dans Horizon Client.

- (Facultatif) Configurez les paramètres de stratégie de groupe **Compte à utiliser pour l'accès non authentifié** et **Se connecter de manière anonyme à l'aide de l'accès non authentifié** pour modifier le comportement de l'accès non authentifié par défaut. Pour plus d'informations, consultez Paramètres de définition de scripts des objets de stratégie de groupe (GPO) des clients.

Procédure

1. Si une connexion VPN est requise, activez le VPN.
2. Démarrez Horizon Client.
3. Cliquez sur le bouton **Options** dans la barre de menus et sélectionnez **Se connecter de manière anonyme à l'aide de l'accès non authentifié**.

   En fonction de la configuration du système client, ce paramètre peut être déjà sélectionné.
4. Connectez-vous au serveur sur lequel vous disposez d'un accès non authentifié.

Option	Action
Se connecter à un nouveau serveur	Double-cliquez sur le bouton **+ Ajouter un serveur** ou cliquez sur le bouton **+ Nouveau serveur** dans la barre de menus, entrez le nom du serveur et cliquez sur **Se connecter**.
Se connecter à un serveur existant	Double-cliquez sur l'icône du serveur dans la fenêtre d'accueil d'Horizon Client.

   Les connexions entre Horizon Client et le serveur utilisent toujours TLS. Le port par défaut pour les connexions TLS est 443. Si le serveur n'est pas configuré pour utiliser le port par défaut, utilisez le format indiqué dans cet exemple : `view.company.com:1443`.

   Il est possible qu'un message de confirmation s'affiche avant l'affichage de la boîte de dialogue Connexion.
5. Lorsque la boîte de dialogue Connexion s'affiche, sélectionnez un compte dans le menu déroulant **Compte d'utilisateur**, si nécessaire.

   Si un seul compte d'utilisateur est disponible, le menu déroulant est désactivé et le compte d'utilisateur est déjà sélectionné.
6. (Facultatif) Si la case **Toujours utiliser ce compte** est disponible, cochez-la pour contourner la boîte de dialogue Connexion lors de votre prochaine connexion au serveur.

   Pour décocher ce paramètre avant votre prochaine connexion au serveur, cliquez avec le bouton droit sur l'icône de serveur sur la fenêtre d'accueil d'Horizon Client et sélectionnez **Oublier le compte d'accès non authentifié enregistré**.
7. Cliquez sur **Connexion** pour vous connecter au serveur.

   La fenêtre de sélection des applications s'affiche.
8. Pour démarrer une application publiée, double-cliquez sur son icône.

Partager des informations d'emplacement

Lorsque la fonctionnalité de redirection de géolocalisation est activée pour un poste de travail distant ou une application publiée, vous pouvez partager les informations d'emplacement du système client avec le poste de travail distant ou l'application publiée.

Pour partager les informations d'emplacement du système client, vous devez configurer un paramètre dans Horizon Client.

Conditions préalables

Un administrateur Horizon doit configurer la fonctionnalité de redirection de géolocalisation pour le poste de travail distant ou l'application publiée.

Cette tâche comprend l'activation de la fonctionnalité de redirection de géolocalisation lorsque vous installez Horizon Agent. Elle comprend également la définition des stratégies de groupe pour configurer les fonctionnalités de redirection de géolocalisation et l'activation du plug-in IE de redirection de géolocalisation de VMware Horizon. Pour plus d'informations sur les exigences, reportez-vous à Configuration système requise pour la redirection de géolocalisation.

Procédure

1. Connectez-vous à un serveur.
2. Ouvrez la boîte de dialogue **Paramètres** et sélectionnez **Géolocalisation** dans le volet de gauche.
   - Cliquez sur l'icône **Paramètres** (engrenage) dans le coin supérieur droit de la fenêtre de sélection des postes de travail et applications.
   - Cliquez avec le bouton droit sur un poste de travail distant ou sur une application publiée de la fenêtre de sélection des postes de travail et des applications et sélectionnez **Paramètres**.

3 Configurez les paramètres de géolocalisation.

Option	Action
Partager des informations d'emplacement du système client avec des postes de travail distants et des applications publiées	Cochez la case **Partager votre emplacement**.
Ne pas afficher la boîte de dialogue Géolocalisation lorsque vous vous connectez à un poste de travail distant ou à une application publiée	Cochez la case **Ne pas afficher la boîte de dialogue lors de la connexion à un poste de travail ou à une application**. La boîte de dialogue Géolocalisation vous demande si vous souhaitez partager des informations d'emplacement avec un poste de travail distant ou une application publiée. Si cette case est décochée, la boîte de dialogue Géolocalisation s'affiche la première fois que vous vous connectez à un poste de travail distant ou à une application publiée. Par exemple, si vous ouvrez une session sur un serveur avant de vous connecter à un poste de travail distant, la boîte de dialogue Géolocalisation s'ouvre. Si vous vous connectez ensuite à un autre poste de travail distant ou à une autre application publiée, cette boîte de dialogue ne s'affiche plus. Pour afficher de nouveau cette boîte de dialogue, vous devez vous déconnecter du serveur, puis rouvrir une session.

4 Cliquez sur **Appliquer** pour enregistrer les modifications.

5 Pour fermer la boîte de dialogue, cliquez sur **OK**.

Masquer la fenêtre VMware Horizon Client

Vous pouvez masquer la fenêtre VMware Horizon Client après avoir ouvert un poste de travail distant ou une application publiée.

Vous pouvez utiliser un paramètre de stratégie de groupe pour indiquer que la fenêtre doit toujours être masquée après l'ouverture d'un poste de travail distant ou d'une application publiée. Pour plus d'informations, reportez-vous à la section Paramètres généraux des objets de stratégie de groupe (GPO) de clients.

Procédure

- Pour masquer la fenêtre VMware Horizon Client après avoir ouvert un poste de travail distant ou une application publiée, cliquez sur le bouton **Fermer** dans le coin de la fenêtre VMware Horizon Client.
- Pour définir un paramètre qui masque toujours la fenêtre VMware Horizon Client après l'ouverture d'un poste de travail distant ou d'une application publiée, avant de vous connecter à un serveur cliquez sur le bouton **Options**, dans la barre de menus puis sélectionnez **Masquer le sélecteur après le lancement d'un élément**.
- Pour afficher la fenêtre VMware Horizon Client après qu'elle a été masquée, cliquez avec le bouton droit sur l'icône VMware Horizon Client dans la barre d'état système, puis sélectionnez **VMware Horizon Client** ou, si vous avez ouvert une session sur un poste de travail distant, cliquez sur le bouton **Options** dans la barre de menus, puis sélectionnez **Passer à un autre poste de travail**.

Reconnexion à un poste de travail distant ou une application publiée

Pour des raisons de sécurité, un administrateur Horizon peut définir des délais d'expiration qui vous déconnectent d'un serveur et verrouillent une application publiée après une certaine période d'inactivité.

Par défaut, vous devez vous connecter à nouveau si Horizon Client est ouvert et que vous êtes connecté à un serveur particulier pendant plus de 10 heures. Ce délai d'expiration s'applique aux connexions aux postes de travail distants et aux applications publiées.

Vous recevez une invite d'avertissement 30 secondes avant qu'une application publiée soit automatiquement verrouillée. Si vous ne répondez pas, l'application publiée est verrouillée. Par défaut, le délai d'expiration survient après 15 minutes d'inactivité, mais un administrateur Horizon peut modifier ce délai d'expiration.

Par exemple, si une ou plusieurs applications publiées sont ouvertes et que vous quittez votre ordinateur, les fenêtres des applications publiées peuvent ne plus être ouvertes lorsque vous revenez une heure plus tard. Une boîte de dialogue peut s'afficher à la place, vous invitant à cliquer sur **OK** pour que les fenêtres des applications publiées s'affichent de nouveau.

Pour configurer ces paramètres de délai d'expiration dans Horizon Console, sélectionnez **Paramètres > Paramètres généraux**, cliquez sur l'onglet **Paramètres généraux**, puis cliquez sur **Modifier**.

Créer un raccourci sur le bureau du Client Windows ou dans le menu Démarrer

Vous pouvez créer un raccourci pour une application publiée ou un poste de travail distant. Le raccourci s'affiche sur le poste de travail du système client, de la même manière que les raccourcis d'applications installées localement. Vous pouvez également créer un raccourci du menu Démarrer de Windows.

Procédure

1. Démarrez Horizon Client et connectez-vous au serveur.
2. Dans la fenêtre de sélection des applications et postes de travail, cliquez avec le bouton droit sur une application publiée ou un poste de travail distant, puis sélectionnez **Créer un raccourci sur le Bureau** ou **Ajouter au menu Démarrer** dans le menu contextuel.

Résultats

En fonction de la commande que vous avez sélectionnée, Horizon Client crée un raccourci sur le poste de travail ou dans le menu Démarrer de Windows sur le système client.

Étape suivante

Vous pouvez renommer, supprimer ou exécuter toute action sur un raccourci que vous pouvez effectuer sur les raccourcis des applications installées localement. Si vous n'êtes pas déjà connecté au serveur lorsque vous utilisez le raccourci, Horizon Client vous invite à vous connecter avant que la fenêtre du poste de travail ou de l'application publiée s'ouvre.

Utilisation des raccourcis créés par le serveur

Un administrateur Horizon peut configurer les raccourcis du menu Démarrer ou les raccourcis de certains postes de travail distants et applications publiées.

Si vous êtes autorisé à vous connecter à un poste de travail distant ou une application publiée qui a des raccourcis, Horizon Client place les raccourcis dans le menu Démarrer, sur le bureau ou les deux sur le système client lorsque vous vous connectez au serveur.

Sur les systèmes Windows 10, Horizon Client place les raccourcis dans la liste Applications. Si un administrateur Horizon crée un dossier de catégorie pour un raccourci, le dossier de catégorie s'affiche sous le dossier Applications de VMware ou en tant que catégorie dans la liste Applications.

Vous pouvez utiliser un paramètre de stratégie de groupe pour configurer si Horizon Client installe automatiquement les raccourcis, invite les utilisateurs finaux avant d'installer les raccourcis ou n'installe jamais les raccourcis. Pour plus d'informations, consultez le paramètre de stratégie de groupe **Installer automatiquement des raccourcis s'ils sont configurés sur Horizon Server** dans Paramètres généraux des objets de stratégie de groupe (GPO) de clients.

Vous pouvez utiliser la commande `vmware-view` avec l'option `-installShortcutsThenQuit` pour créer un script qui s'exécute lorsque le système client démarre et installe des raccourcis automatiquement. Pour plus d'informations, reportez-vous à la section Utilisation des commandes Horizon Client.

Si vous n'êtes pas déjà connecté au serveur lorsque vous cliquez sur un raccourci créé par le serveur, Horizon Client vous invite à vous connecter avant que le poste de travail ou l'application s'ouvre.

Si un administrateur Horizon modifie les raccourcis d'application publiée et de poste de travail distant sur le serveur, les raccourcis sont mis à jour sur le système client par défaut la prochaine fois que vous vous connectez à ce serveur. Vous pouvez modifier le comportement de mise à jour des raccourcis dans Horizon Client. Pour plus d'informations, reportez-vous à la section Configurer les mises à jour des raccourcis du menu Démarrer.

Pour supprimer les raccourcis de serveur créés à partir du système client, vous pouvez supprimer le serveur depuis la fenêtre de sélection des serveurs Horizon Client ou désinstaller Horizon Client.

Note Les utilisateurs ne sont pas invités à installer des raccourcis créés par le serveur et les raccourcis créés par le serveur ne sont pas créés sur des clients en mode kiosque.

Configurer les mises à jour des raccourcis du menu Démarrer

Vous pouvez définir si les modifications apportées aux raccourcis d'application publiée ou de poste de travail distant sur le serveur sont appliquées ou non au système client lorsque vous vous connectez au serveur.

Conditions préalables

Vous ne pouvez pas modifier le paramètre de mise à jour des raccourcis, sauf si vous avez déjà installé un raccourci à partir d'un serveur.

Procédure

1. Démarrez Horizon Client et connectez-vous à un serveur.
2. Ouvrez la boîte de dialogue Paramètres et sélectionnez **Raccourcis**.
   - Cliquez sur l'icône **Paramètres** (engrenage) dans le coin supérieur droit de la fenêtre de sélection des postes de travail et applications.
   - Cliquez-avec le bouton droit sur l'icône d'un poste de travail distant ou d'une application publiée et sélectionnez **Paramètres**.
3. Cochez ou décochez la case **Mettre à jour automatiquement la liste des raccourcis de poste de travail et d'application** et cliquez sur **OK**.

Configurer la fonction de connexion automatique pour un poste de travail distant

Vous pouvez configurer un serveur de manière à ouvrir un poste de travail distant spécifique automatiquement lorsque vous vous y connectez. Vous ne pouvez pas configurer de serveur pour ouvrir une application publiée automatiquement.

Conditions préalables

Procurez-vous les informations d'identification pour vous connecter au serveur, telles que le nom d'utilisateur et le mot de passe, le nom d'utilisateur et le code secret RSA SecurID, le nom d'utilisateur et le code secret pour l'authentification RADIUS ou le numéro d'identification personnel (PIN) de carte à puce.

Procédure

1. Démarrez Horizon Client et connectez-vous au serveur.
2. Dans la fenêtre de sélection des postes de travail et applications, cliquez avec le bouton droit sur le poste de travail distant, puis sélectionnez **Se connecter automatiquement à ce poste de travail**.
3. Cliquez sur **Appliquer** pour enregistrer les modifications.
4. Pour fermer la boîte de dialogue, cliquez sur **OK**.
5. Déconnectez-vous du serveur.

6 Reconnectez-vous au serveur.

Horizon Client lance automatiquement le poste de travail distant.

7 (Facultatif) Si vous devez désactiver la fonctionnalité de connexion automatique pour le poste de travail distant, cliquez sur le menu déroulant **Options** dans la barre de menus du poste de travail distant et désélectionnez l'option **Se connecter automatiquement à ce poste de travail**.

Fermer une session ou se déconnecter

Si vous vous déconnectez d'un poste de travail distant sans fermer la session, les applications du poste de travail distant peuvent rester ouvertes. Vous pouvez également vous déconnecter d'un serveur tout en gardant des applications publiées en cours d'exécution.

Vous pouvez fermer une session depuis un poste de travail distant, même si vous n'avez aucun poste de travail distant ouvert. Cette fonctionnalité revient à envoyer Ctrl+Alt+Suppr au poste de travail distant et à sélectionner **Fermer la session**.

Note La combinaison de touches Windows Ctrl+Alt+Suppr n'est pas prise en charge sur les postes de travail distants. À la place, cliquez sur le bouton **Envoyer Ctrl+Alt+Suppr** dans la barre de menus. Vous pouvez également appuyer sur Ctrl+Alt+Inser.

Procédure

- Se déconnecter d'un poste de travail distant sans fermer la session.

Option	Action
Dans la fenêtre du poste de travail distant	effectuez l'une des opérations suivantes : ■ Cliquez sur le bouton **Fermer** dans le coin de la fenêtre du poste de travail distant. ■ Sélectionnez **Options > Se déconnecter** dans la barre de menus de la fenêtre du poste de travail distant.
Depuis la fenêtre de sélection des postes de travail et applications	Dans le coin supérieur gauche de la fenêtre de sélection des postes de travail et applications, cliquez sur l'icône **Se déconnecter de ce serveur**, puis cliquez sur **OK** dans la boîte de dialogue d'avertissement. Si vous n'êtes pas autorisé à utiliser plusieurs postes de travail distants ou plusieurs applications publiées sur le serveur, la fenêtre de sélection des postes de travail et applications est ouverte.

Note Un administrateur Horizon peut configurer des postes de travail distants pour fermer automatiquement la session lorsqu'ils sont déconnectés. Dans ce cas, toutes les applications ouvertes sur le poste de travail distant sont fermées.

- Fermer une session et se déconnecter d'un poste de travail distant.

Option	Action
Depuis le poste de travail distant	Utilisez le menu **Démarrer** de Windows pour fermer la session.
À partir de la barre de menus	Sélectionnez **Options > Se déconnecter et fermer une session**. Si vous utilisez cette procédure, les fichiers ouverts sur le poste de travail distant sont fermés sans être enregistrés.

- Se déconnecter d'une application publiée.

Option	Action
Se déconnecter de l'application publiée mais pas du serveur	Quittez l'application publiée de la façon habituelle, par exemple, en cliquant sur le bouton **Fermer** dans le coin de la fenêtre d'application.
Se déconnecter de l'application publiée et du serveur	Dans le coin supérieur gauche de la fenêtre de sélection des applications, cliquez sur l'icône **Se déconnecter de ce serveur**, puis cliquez sur **OK** dans la boîte de dialogue d'avertissement.
Fermer la fenêtre de sélection des applications mais laisser l'application publiée s'exécuter	Cliquez sur le bouton **Fermer**. La fenêtre de sélection des applications se ferme.

- Fermez la session lorsqu'aucun poste de travail distant n'est ouvert.

  Si vous utilisez cette procédure, les fichiers ouverts sur le poste de travail distant sont fermés sans être enregistrés.

  a Démarrez Horizon Client, connectez-vous au serveur qui fournit l'accès au poste de travail distant et entrez vos informations d'identification pour l'authentification.

  b Cliquez avec le bouton droit sur l'icône du poste de travail distant, puis sélectionnez **Fermer la session**.

Déconnexion d'un serveur

Lorsque vous n'utilisez plus un poste de travail distant ou une application publiée, vous pouvez vous déconnecter du serveur.

Pour vous déconnecter d'un serveur, cliquez sur l'icône **Se déconnecter de ce serveur**, située dans le coin supérieur gauche de la fenêtre Horizon Client, ou appuyez sur Alt+D.

Travailler dans une application publiée ou un poste de travail distant

5

Horizon Client pour Windows fournit un environnement de poste de travail et d'application familier et personnalisé. Les utilisateurs finaux peuvent accéder à des périphériques USB et autres connectés à leur ordinateur Windows local, envoyer des documents à une imprimante pouvant être détectée par leur ordinateur local, s'authentifier avec des cartes à puce et utiliser plusieurs écrans.

Ce chapitre contient les rubriques suivantes :

- Prise en charge des fonctionnalités pour les clients Windows
- Redimensionnement de la fenêtre du poste de travail distant
- Écrans et résolution d'écran
- Utiliser des périphériques USB
- Utilisation de webcams et de microphones
- Sélectionner un haut-parleur préféré pour un poste de travail distant
- Partage de sessions de poste de travail distant
- Partager des lecteurs et des dossiers locaux
- Ouvrir les fichiers locaux dans des applications publiées
- Copier et coller
- Glisser-déposer
- Conseils pour l'utilisation d'applications publiées
- Impression à partir d'un poste de travail distant ou d'une application publiée
- Améliorer les performances de la souris sur un poste de travail distant
- Utilisation de scanners
- Redirection des ports série
- Raccourcis clavier
- Synchronisation de la langue source d'entrée du clavier
- Configurer la synchronisation des touches de verrouillage

Prise en charge des fonctionnalités pour les clients Windows

Certains systèmes d'exploitation invités et fonctionnalités de poste de travail distant nécessitent des versions d'Horizon Agent spécifiques. Utilisez ces informations pour planifier les fonctionnalités à mettre à la disposition de vos utilisateurs finaux.

Postes de travail virtuels Windows pris en charge

Les postes de travail virtuels Windows sont des machines virtuelles à session unique.

Cette version de Horizon Client fonctionne avec les postes de travail virtuels Windows sur lesquels Horizon Agent 7.5 ou version ultérieure est installé. Les systèmes d'exploitation invités pris en charge incluent Windows 7, Windows 8.x, Windows 10, Windows Server 2012 R2, Windows Server 2016 et Windows Server 2019, avec les limitations suivantes :

- Les postes de travail virtuels Windows Server 2019 requièrent Horizon Agent 7.7 ou version ultérieure.
- Les postes de travail virtuels Windows 7 et Windows 8.x ne sont pas pris en charge avec Horizon Agent 2006 et versions ultérieures.

Postes de travail publiés sur des hôtes RDS pris en charge

Les hôtes RDS sont des ordinateurs serveurs sur lesquels les services Bureau à distance Windows et Horizon Agent sont installés. Plusieurs utilisateurs peuvent avoir plusieurs sessions simultanées de poste de travail publiées sur un hôte RDS. Un hôte RDS peut être une machine physique ou une machine virtuelle.

Cette version de Horizon Client fonctionne avec les hôtes RDS sur lesquels Horizon Agent 7.5 ou version ultérieure est installé. Les systèmes d'exploitation invités pris en charge incluent Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 et Windows Server 2019, avec les limitations suivantes :

- Les hôtes RDS Windows Server 2019 requièrent Horizon Agent 7.7 ou version ultérieure.
- Les hôtes RDS de Windows Server 2012 ne sont pas pris en charge avec Horizon Agent 2006 et versions ultérieures.

Conditions requises pour les fonctionnalités spécifiques de poste de travail distant

La plupart des fonctionnalités de poste de travail distant fonctionnent avec Horizon Agent 7.5, mais certaines fonctionnalités nécessitent des versions ultérieures d'Horizon Agent.

Fonctionnalité	Configuration requise
Faire glisser du texte et des images	Horizon Agent 7.9 ou version ultérieure
Faire glisser des fichiers et des dossiers	Horizon Agent 7.7 ou version ultérieure
Redirection de géolocalisation	Horizon Agent 7.6 ou version ultérieure

Fonctionnalité	Configuration requise
Redirection de navigateur	Horizon Agent 7.10 ou version ultérieure
VMware Integrated Printing et impression basée sur l'emplacement	Horizon Agent 7.7 ou version ultérieure

Cette version d'Horizon Client de Windows ne prend pas en charge les fonctionnalités suivantes de poste de travail distant, qui sont prises en charge dans les versions 7.x d'Horizon Agent :

- Impression virtuelle (également appelée ThinPrint)
- Redirection d'URL Flash
- redirection Flash

Postes de travail Linux pris en charge

Pour obtenir la liste des systèmes d'exploitation invités Linux pris en charge et pour plus d'informations sur les fonctionnalités prises en charge, consultez le document *Configuration des postes de travail Linux dans Horizon*.

Redimensionnement de la fenêtre du poste de travail distant

Si vous faites glisser un coin de la fenêtre du poste de travail distant pour la redimensionner, une info-bulle affiche la résolution de l'écran dans le coin inférieur droit de la fenêtre.

Si vous utilisez le protocole d'affichage VMware Blast ou PCoIP, l'info-bulle change pour afficher des résolutions d'écran différentes lorsque vous modifiez la taille de la fenêtre du poste de travail distant. Ces informations sont utiles si vous devez redimensionner la fenêtre du poste de travail distant à une résolution spécifique.

Si un administrateur Horizon a verrouillé la taille de l'invité, ou si vous utilisez le protocole d'affichage RDP, vous ne pouvez pas modifier la résolution de la fenêtre du poste de travail distant. Dans ces cas-là, l'info-bulle de résolution indique la résolution initiale.

Si vous disposez de plusieurs moniteurs, vous pouvez sélectionner les moniteurs sur lesquels afficher une fenêtre de poste de travail distant. Pour plus d'informations, reportez-vous à la section Sélectionner des moniteurs spécifiques pour afficher un poste de travail distant. Vous pouvez également configurer la fenêtre du poste de travail distant pour qu'elle s'ouvre sur un seul moniteur. Pour plus d'informations, reportez-vous à la section Afficher un poste de travail distant sur un seul moniteur dans une configuration à plusieurs moniteurs.

Écrans et résolution d'écran

Vous pouvez étendre un poste de travail distant ou une application publiée sur plusieurs moniteurs. Si vous disposez d'un moniteur haute résolution, vous pouvez afficher l'application publiée ou le poste de travail distant en pleine résolution.

Configurations à plusieurs moniteurs prises en charge

Horizon Client prend en charge les configurations à plusieurs moniteurs suivantes :

- À partir d'Horizon 7 version 7.8, six moniteurs à une résolution de 2560 X 1600 avec des postes de travail virtuels qui exécutent Windows 10 version 1703 ou ultérieure sont pris en charge. Les spécifications d'affichage Windows mises à jour nécessitent Windows 10 version 1803 ou ultérieure pour la prise en charge de six moniteurs sur Horizon 7 version 7.9 et ultérieures.
- Avec les pools de postes de travail d'Instant Clone, le nombre maximal de moniteurs est de quatre à la résolution 4K.
- Avec deux moniteurs ou plus, il n'est pas nécessaire qu'ils soient dans le même mode. Par exemple, si vous utilisez un ordinateur portable connecté à un moniteur externe, le moniteur externe peut être en mode portrait ou en mode paysage.
- Avec la version matérielle 13 ou version antérieure, les moniteurs peuvent être placés côte à côte, associés deux par deux ou empilés verticalement, seulement si vous utilisez deux moniteurs et si la hauteur totale est inférieure à 4 096 pixels.
- Pour utiliser la fonctionnalité de plusieurs moniteurs sélective, vous devez utiliser le protocole d'affichage VMware Blast ou PCoIP. Pour plus d'informations, consultez Sélectionner des moniteurs spécifiques pour afficher un poste de travail distant et Sélectionner des moniteurs spécifiques pour afficher les applications publiées.
- Pour utiliser la fonction de rendu 3D vSGA, vous devez utiliser le protocole d'affichage VMware Blast ou PCoIP. Vous pouvez utiliser deux moniteurs maximum, avec une résolution maximale de 1 920 x 1 200. Pour une résolution de 4K (3 840 x 2 160), un seul moniteur est pris en charge.
- Pour vGPU ou les autres modes de relais GPU, le matériel et les pilotes du fournisseur déterminent le nombre de moniteurs et la résolution maximale. Pour plus d'informations, consultez le *Guide d'utilisateur de GPU virtuel NVIDIA GRID* ou visitez le site Web du fournisseur.
- Si vous utilisez cinq moniteurs ou plus et que vous vous connectez à une session distante avec VMware Blast, la connexion initiale à la nouvelle session échoue si vous utilisez les mêmes informations d'identification utilisateur pour vos connecter à la session avec PCoIP depuis un autre périphérique (sans fermer la session d'origine).
- Avec le protocole d'affichage VMware Blast, une résolution d'écran de poste de travail distant de 8 000 pixels (7680 x 4320) est prise en charge. Deux affichages de 8 000 pixels sont pris en charge. La version matérielle de la machine virtuelle de poste de travail doit être 14 (ESXi 6.7 ou version ultérieure). Vous devez allouer suffisamment de ressources système sur la machine virtuelle pour prendre en charge un affichage de 8 000 pixels. Pour plus d'informations sur les configurations de moniteur prises en charge pour les postes de travail basés sur GRID et pour les profils de vGPU NVIDIA, reportez-vous au *Guide de l'utilisateur du logiciel des GPU virtuels* sur le site Web de NVIDIA. Cette fonctionnalité n'est prise en charge qu'avec le client Windows.

- Avec le protocole d'affichage VMware Blast ou PCoIP, la résolution d'écran de poste de travail distant de 4K (3 840 x 2 160) est prise en charge. Le nombre d'écrans 4K pris en charge dépend de la version matérielle de la machine virtuelle de poste de travail et de la version de Windows.

Version du matériel	Version Windows	Nombre d'écrans 4K pris en charge
10 (compatible avec ESXi 5.5.x)	7, 8, 8.x, 10	1
11 (compatible avec ESXi 6.0)	7 (fonction de rendu 3D désactivée et Windows Aero désactivé)	3
11	7 (fonction de rendu 3D activée)	1
11	8, 8.x, 10	1
13 ou 14	7, 8, 8.x, 10 (fonction de rendu 3D activée)	1
13 ou 14	7, 8, 8.x, 10	4

  Pour optimiser les performances, la machine virtuelle doit disposer d'au moins 2 Go de RAM et de 2 vCPU. Cette fonction peut nécessiter de bonnes conditions de réseau, telles qu'une bande passante de 1 000 Mbit/s avec une faible latence du réseau et un taux de perte de paquets réduit.

  Note Lorsque la résolution d'écran de poste de travail distant est définie sur 3 840 x 2 160 (4K), les éléments sur l'écran peuvent sembler plus petits, et il peut vous être impossible d'utiliser la boîte de dialogue Résolution d'écran sur le poste de travail distant pour agrandir le texte et les autres éléments. Dans ce scénario, vous pouvez définir le DPI de la machine cliente sur le paramètre approprié et activer la fonctionnalité de synchronisation DPI afin de rediriger le paramètre DPI de la machine cliente vers le poste de travail distant.

- Si vous disposez de Microsoft RDP 7, vous pouvez utiliser un maximum de 16 moniteurs pour afficher un poste de travail distant.
- Si vous utilisez le protocole d'affichage Microsoft RDP, Connexion Bureau à distance Microsoft (RDC) 6.0 ou version ultérieure doit être installé sur le poste de travail distant.

Sélectionner des moniteurs spécifiques pour afficher un poste de travail distant

Si vous disposez de plusieurs moniteurs, vous pouvez sélectionner les moniteurs sur lesquels afficher une fenêtre de poste de travail distant. Par exemple, si vous disposez de deux moniteurs, vous pouvez spécifier que la fenêtre de poste de travail distant n'apparaît que sur un de ces moniteurs.

À partir d'Horizon 7 version 7.8, vous pouvez sélectionner jusqu'à six moniteurs adjacents avec des postes de travail virtuels qui exécutent Windows 10 version 1703 et ultérieures. À partir d'Horizon 7 version 7.9, vous pouvez sélectionner jusqu'à six moniteurs adjacents avec des postes de travail virtuels qui exécutent Windows 10 version 1803 et ultérieures. Les moniteurs peuvent être placés côte à côte ou l'un sur l'autre. Par exemple, vous pouvez configurer deux rangées de trois moniteurs chaque. Avec les autres versions de Windows ou les versions antérieures de VMware Horizon, vous pouvez utiliser jusqu'à quatre moniteurs adjacents.

Conditions préalables

Vous devez disposer d'au moins deux moniteurs.

Procédure

1. Démarrez Horizon Client et connectez-vous à un serveur.
2. Ouvrez la boîte de dialogue Paramètres pour le poste de travail distant.
   - Cliquez sur l'icône **Paramètres** (engrenage) dans le coin supérieur droit de la fenêtre de sélection des postes de travail et applications, puis sélectionnez le poste de travail distant dans le volet de gauche.
   - Cliquez avec le bouton droit sur le poste de travail distant de la fenêtre de sélection des postes de travail et applications et sélectionnez **Paramètres**.
3. Sélectionnez **PCoIP** ou **VMware Blast** dans le menu déroulant **Se connecter via**.

   Le menu déroulant **Connecter via** s'affiche uniquement si un administrateur Horizon l'a activé.
4. Dans le menu déroulant **Afficher**, sélectionnez **Tous les moniteurs**.

   Les miniatures des moniteurs actuellement connectés au système client s'affichent sous Paramètres d'affichage. La topologie d'affichage correspond aux paramètres d'affichage sur le système client.
5. Pour sélectionner ou désélectionner un moniteur sur lequel vous souhaitez afficher la fenêtre de poste de travail distant, cliquez sur une miniature.

   Lorsque vous sélectionnez un moniteur, sa miniature change de couleur. Si vous enfreignez une règle de sélection d'affichage, un message d'avertissement s'affiche.
6. Cliquez sur **Appliquer** pour enregistrer les modifications.
7. Pour fermer la boîte de dialogue, cliquez sur **OK**.
8. Connectez-vous au poste de travail distant.

   Vos modifications s'appliquent immédiatement lorsque vous vous connectez au poste de travail distant. Horizon Client enregistre les paramètres d'affichage dans un fichier de préférences du poste de travail distant après avoir quitté Horizon Client.

Afficher un poste de travail distant sur un seul moniteur dans une configuration à plusieurs moniteurs

Si vous disposez de plus de deux moniteurs, mais que vous voulez qu'une fenêtre de poste de travail distant n'apparaisse que sur un seul moniteur, vous pouvez configurer la fenêtre de poste de travail distant pour qu'elle s'ouvre sur un seul moniteur.

Conditions préalables

Vous devez disposer d'au moins deux moniteurs.

Procédure

1. Démarrez Horizon Client et connectez-vous à un serveur.
2. Ouvrez la boîte de dialogue Paramètres pour le poste de travail distant.
   - Cliquez sur l'icône **Paramètres** (engrenage) dans le coin supérieur droit de la fenêtre de sélection des postes de travail et applications, puis sélectionnez le poste de travail distant dans le volet de gauche.
   - Cliquez avec le bouton droit sur le poste de travail distant de la fenêtre de sélection des postes de travail et applications et sélectionnez **Paramètres**.
3. Dans le menu déroulant **Connecter via**, sélectionnez **PCoIP** ou **VMware Blast**.

   Le menu déroulant **Connecter via** s'affiche uniquement si un administrateur Horizon l'a activé.
4. Dans le menu déroulant **Affichage**, sélectionnez **Plein écran**, **Fenêtre - Grande**, **Fenêtre - Petite** ou **Personnalisé**.

   Fenêtre - Grande définit la taille de fenêtre sur 1 904 x 978 pixels. **Fenêtre - Petite** définit la taille de fenêtre de 640 x 480 pixels. Si vous sélectionnez **Personnalisé**, vous pouvez sélectionner une taille de fenêtre spécifique.
5. Cliquez sur **Appliquer** pour enregistrer les modifications.
6. Pour fermer la boîte de dialogue, cliquez sur **OK**.

Résultats

Par défaut, la fenêtre de poste de travail distant s'ouvre sur le moniteur principal. Vous pouvez faire glisser la fenêtre de poste de travail distant vers un écran secondaire et, lors de la prochaine ouverture du poste de travail distant, la fenêtre de poste de travail distant s'affichera sur ce moniteur. La fenêtre s'ouvre, est centrée dans le moniteur et utilise la taille de fenêtre que vous avez sélectionnée pour le mode d'affichage, pas une taille que vous pouvez avoir créée en faisant glisser la fenêtre pour la redimensionner.

Sélectionner des moniteurs spécifiques pour afficher les applications publiées

Si vous disposez d'au moins deux moniteurs, vous pouvez sélectionner les moniteurs sur lesquels afficher les fenêtres des applications publiées. Par exemple, si vous disposez de deux moniteurs,

vous pouvez spécifier que les fenêtres des applications publiées n'apparaissent que sur un de ces moniteurs.

Vous pouvez sélectionner jusqu'à quatre moniteurs adjacents. Les moniteurs peuvent être placés les uns à côté des autres, empilés deux par deux ou empilés à la verticale. Deux moniteurs au maximum peuvent être empilés à la verticale.

Conditions préalables

Vous devez disposer d'au moins deux moniteurs.

Procédure

1. Démarrez Horizon Client et connectez-vous à un serveur.
2. Ouvrez la boîte de dialogue Paramètres pour les applications publiées.
   - Cliquez sur l'icône **Paramètres** (engrenage) dans le coin supérieur droit de la fenêtre de sélection des postes de travail et applications, puis sélectionnez **Applications**.
   - Cliquez avec le bouton droit sur une application publiée de la fenêtre de sélection des postes de travail et applications et sélectionnez **Paramètres**.
3. Sous Paramètres d'affichage, sélectionnez ou désélectionnez un moniteur sur lequel vous voulez afficher la fenêtre de l'application publiée.

   Lorsque vous sélectionnez un moniteur, sa miniature change de couleur. Si vous enfreignez une règle de sélection d'affichage, un message d'avertissement s'affiche.
4. Cliquez sur **Appliquer** pour enregistrer les modifications.
5. Pour fermer la boîte de dialogue, cliquez sur **OK**.

Utiliser la mise à l'échelle de l'affichage

En général, les utilisateurs qui ont une vue faible ou qui disposent d'écrans haute résolution, comme des écrans 4K, activent la mise à l'échelle en définissant le DPI (points par pouce) sur le système client sur une valeur supérieure à 100 %. Le paramètre DPI contrôle la taille du texte, des applications et des icônes. Un paramètre DPI inférieur les fait apparaître plus petits et un paramètre supérieur les fait apparaître plus grands. Avec la fonctionnalité de mise à l'échelle de l'affichage, les applications publiées et les postes de travail distants prennent en charge le paramètre de mise à l'échelle du système client et s'affichent avec une taille normale plutôt qu'en très petit.

Horizon Client compare le paramètre DPI qu'il reçoit du poste de travail distant ou de l'application publiée au paramètre DPI du système client. Si les paramètres DPI ne correspondent pas et si la fonctionnalité de mise à l'échelle de l'affichage est activée, Horizon Client calcule le facteur d'échelle. Par exemple, si le paramètre DPI d'un poste de travail distant est de 100 % et si le paramètre DPI du système client est de 200 %, Horizon Client augmente la capacité du paramètre DPI du poste de travail distant par un facteur de 2 (200/100 = 2).

Horizon Client enregistre le paramètre de mise à l'échelle de l'affichage pour chaque poste de travail distant séparément. Le paramètre de mise à l'échelle de l'affichage s'applique à toutes les applications publiées qui sont disponibles pour l'utilisateur actuellement connecté.

Dans une configuration à plusieurs moniteurs, l'utilisation de la mise à l'échelle de l'affichage n'affecte pas les résolutions maximales ni le nombre de moniteurs pris en charge par Horizon Client. Lorsque la mise à l'échelle de l'affichage est autorisée et effective, elle est basée sur le paramètre DPI du système client.

Vous pouvez masquer le paramètre de mise à l'échelle de l'affichage en activant le paramètre de stratégie de groupe **Taille d'invité verrouillée** d'Horizon Client.

Vous pouvez activer ou désactiver la mise à l'échelle de l'affichage pour l'ensemble des postes de travail distants et des applications publiées en définissant le paramètre de stratégie de groupe **Autoriser la mise à l'échelle de l'affichage**. Pour plus d'informations, reportez-vous à la section Paramètres généraux des objets de stratégie de groupe (GPO) de clients. L'option **Autoriser la mise à l'échelle de l'affichage** est activée par défaut et cochée dans l'interface utilisateur.

Cette procédure décrit comment activer la fonctionnalité de mise à l'échelle de l'affichage avant de vous connecter à un poste de travail distant ou à une application publiée. Vous pouvez activer la fonctionnalité de mise à l'échelle de l'affichage une fois que vous êtes connecté à un poste de travail distant en sélectionnant **Options > Autoriser la mise à l'échelle de l'affichage** dans la barre de menus d'Horizon Client.

Procédure

1. Démarrez Horizon Client et connectez-vous à un serveur.
2. Dans la fenêtre de sélection des postes de travail et applications, cliquez avec le bouton droit sur l'application publiée ou le poste de travail distant et sélectionnez **Paramètres**.
3. Cochez la case **Autoriser la mise à l'échelle de l'affichage**.

   Si un administrateur a préconfiguré la mise à l'échelle de l'affichage, la case à cocher est grisée. Si un administrateur a masqué le paramètre de mise à l'échelle de l'affichage, la case à cocher ne s'affiche pas.
4. Cliquez sur **Appliquer** pour enregistrer les modifications.
5. Pour fermer la boîte de dialogue, cliquez sur **OK**.

Utilisation de la synchronisation DPI

La fonctionnalité de synchronisation DPI garantit que le paramètre DPI d'un poste de travail distant ou d'une application publiée correspond au paramètre DPI du système client.

Comme la fonctionnalité de mise à l'échelle de l'affichage, la fonctionnalité de synchronisation DPI peut améliorer la lisibilité du texte et des icônes sur des affichages haute résolution. Contrairement à la fonctionnalité de mise à l'échelle de l'affichage, qui augmente la taille des polices et des images, et qui peut les rendre floues, la fonctionnalité de synchronisation DPI augmente la taille des polices et des images, en les gardant nettes. Pour cette raison, la fonctionnalité de synchronisation DPI est généralement préférée pour une expérience utilisateur optimale.

Si la fonctionnalité de synchronisation DPI et la fonctionnalité de mise à l'échelle de l'affichage sont toutes deux activées, une seule fonctionnalité prend effet.

Le paramètre de stratégie du groupe de l'agent **Synchronisation DPI** détermine si la fonctionnalité de synchronisation DPI est activée ou non. Cette fonctionnalité est activée par défaut.

Comportement de la synchronisation DPI avec des postes de travail distants

Le comportement de synchronisation DPI par défaut dépend de la version d'Horizon Agent installée sur la machine agent.

À partir de Horizon Agent 2012, le paramètre DPI par moniteur du client est synchronisé avec l'agent, et, par défaut, les modifications prennent effet immédiatement lors d'une session distante. Cette fonctionnalité est contrôlée par le paramètre de stratégie de groupe de l'agent **Synchronisation DPI par moniteur**. La fonctionnalité de synchronisation DPI par moniteur est prise en charge par défaut pour les postes de travail virtuels et physiques. Elle n'est pas pris en charge pour les postes de travail publiés.

Avec les versions antérieures d'Horizon Agent, Horizon Client ne prend en charge que la synchronisation avec le paramètre DPI système. La synchronisation DPI se produit lors de la connexion initiale. La mise à l'échelle de l'affichage fonctionne alors en cas de reconnexion, si nécessaire. Lorsque la synchronisation DPI fonctionne et que le paramètre DPI du système client correspond au paramètre DPI du poste de travail distant, la mise à l'échelle de l'affichage ne peut pas être appliquée, même si vous sélectionnez l'option **Autoriser la mise à l'échelle de l'affichage** dans l'interface utilisateur. Windows n'autorise pas les utilisateurs à modifier le paramètre DPI au niveau du système pour la session utilisateur actuelle, et la synchronisation DPI ne se produit que lorsqu'ils se connectent et démarrent une session distante. Si les utilisateurs modifient le paramètre DPI au cours d'une session distante, ils doivent se déconnecter, puis se reconnecter pour que le paramètre DPI du poste de travail distant corresponde au nouveau paramètre DPI du système client.

Le paramètre DPI de l'agent se trouve dans le Registre Windows sur `Computer\HKEY_CURRENT_USER\Control Panel\Desktop: logPixels`.

Note Celui-ci doit être différent du paramètre DPI du moniteur principal. Par exemple, si vous fermez le moniteur principal et si le système bascule vers un écran externe qui dispose d'un paramètre DPI différent de celui du moniteur principal, le paramètre DPI système est toujours le même que le paramètre DPI du moniteur principal précédemment fermé.

Cette version d'Horizon Client ne prend pas en charge le paramètre de stratégie de groupe de l'agent **Synchronisation DPI par connexion**, qui est livré avec Horizon Agent versions 7.8 à 2006.

Pour plus d'informations sur les paramètres de stratégie de groupe de synchronisation DPI, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon* de votre version de Horizon Agent.

Systèmes d'exploitation invités pris en charge pour les postes de travail virtuels

Pour les postes de travail virtuels, la fonctionnalité de synchronisation DPI est prise en charge sur les systèmes d'exploitation invités suivants :

- Windows 7 32 ou 64 bits
- Windows 8.x 32 ou 64 bits
- Windows 10 32 ou 64 bits
- Windows Server 2008 R2 configuré en tant que poste de travail
- Windows Server 2012 R2 configuré en tant que poste de travail
- Windows Server 2016 configuré en tant que poste de travail
- Windows Server 2019 configuré en tant que poste de travail

Note Pour les machines Windows Server configurées en tant que poste de travail, la fonctionnalité de synchronisation DPI par moniteur n'est pas prise en charge.

Hôtes RDS pris en charge pour les postes de travail publiés et les applications publiées

Pour les applications et les postes de travail publiés, la fonctionnalité de synchronisation DPI est prise en charge sur les hôtes RDS suivants :

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

Note Pour les hôtes RDS, la fonctionnalité de synchronisation DPI par moniteur n'est pas prise en charge. Cette limitation ne s'applique pas aux applications publiées qui s'exécutent sur des pools de postes de travail avec la fonctionnalité d'applications hébergées de machine virtuelle.

Modifier le mode d'affichage d'un poste de travail distant

Vous pouvez modifier le mode d'affichage, en basculant par exemple du mode **Tous les moniteurs** sur le mode **Plein écran**, avant ou après vous être connecté à un poste de travail distant. Cette fonctionnalité n'est pas prise en charge pour les applications publiées.

Procédure

1 Démarrez Horizon Client et connectez-vous à un serveur.

2 Ouvrez la boîte de dialogue Paramètres pour le poste de travail distant.

- Cliquez sur l'icône **Paramètres** (engrenage) dans le coin supérieur droit de la fenêtre de sélection des postes de travail et applications, puis sélectionnez le poste de travail distant dans le volet de gauche.
- Cliquez avec le bouton droit sur le poste de travail distant de la fenêtre de sélection des postes de travail et applications et sélectionnez **Paramètres**.

3 Dans le menu déroulant **Affichage** , sélectionnez le mode d'affichage.

Option	Description
Tous les moniteurs	Affiche la fenêtre du poste de travail distant sur plusieurs moniteurs. La fenêtre du poste de travail distant s'affiche sur tous les moniteurs par défaut.
Plein écran	La fenêtre du poste de travail distant occupe tout l'écran.
Fenêtre - Grande	Définit la taille de la fenêtre du poste de travail distant sur 1904 x 978 pixels.
Fenêtre - Petite	Définit la taille de la fenêtre du poste de travail distant sur 640 x 480 pixels.
Personnalisé	Affiche un curseur que vous pouvez utiliser pour configurer une taille personnalisée pour la fenêtre du poste de travail distant.

4 Cliquez sur **Appliquer** pour enregistrer les modifications.

5 Pour fermer la boîte de dialogue, cliquez sur **OK**.

Si vous êtes connecté au poste de travail à distance, vos modifications sont appliquées immédiatement. Si vous n'êtes pas connecté au poste de travail distant, vos modifications sont appliquées lorsque vous vous connectez à celui-ci. Horizon Client enregistre les paramètres d'affichage dans un fichier de préférences du poste de travail distant après avoir quitté Horizon Client.

Résultats

Si vous utilisez le mode **Tous les moniteurs** et que vous cliquez sur le bouton **Réduire**, si vous agrandissez ensuite la fenêtre, elle repasse en mode **Tous les moniteurs**. De la même façon, si vous utilisez le mode **Plein écran** et réduisez la fenêtre, si vous l'agrandissez ensuite, elle repasse en mode **Plein écran** sur le moniteur.

Note Si Horizon Client utilise tous les moniteurs et si vous agrandissez la fenêtre d'une application publiée, la fenêtre passe en plein écran uniquement sur le moniteur qui la contient.

Personnaliser la résolution et la mise à l'échelle de l'affichage pour un poste de travail distant

Vous pouvez utiliser Horizon Client pour personnaliser la résolution et la mise à l'échelle de l'affichage d'un poste de travail distant. La résolution d'affichage détermine la clarté du texte et des images. À des résolutions supérieures, telles que 1600 x 1200 pixels, l'apparence

des éléments est plus nette. La mise à l'échelle de l'affichage, qui est représentée par un pourcentage, augmente ou diminue la taille du texte, des icônes et des éléments de navigation.

Par défaut, les paramètres personnalisés de résolution d'affichage et de mise à l'échelle de l'affichage ne sont stockés que sur le système client local. Un administrateur peut utiliser le paramètre de stratégie de groupe **Enregistrer la résolution et le paramètre DPI sur le serveur** pour enregistrer ces paramètres sur le serveur afin qu'ils soient toujours appliqués, quel que soit le périphérique client que vous utilisez pour vous connecter au poste de travail distant. Pour plus d'informations, reportez-vous à la section Paramètres généraux des objets de stratégie de groupe (GPO) de clients.

Cette fonctionnalité présente les limitations et considérations suivantes.

- La personnalisation de la résolution et de la mise à l'échelle de l'affichage d'un poste de travail distant n'est pas prise en charge en mode Plusieurs moniteurs.
- Si vous sélectionnez une résolution personnalisée supérieure ou inférieure à celle du client, Horizon Client redimensionne la fenêtre du poste de travail distant pour qu'elle s'ajuste à la fenêtre du client.
- Si vous personnalisez la résolution d'affichage lors d'une session de poste de travail distant, vos modifications prennent effet immédiatement. Si vous personnalisez la mise à l'échelle de l'affichage lors d'une session de poste de travail distant, vous devez vous déconnecter, puis vous reconnecter pour que vos modifications prennent effet.
- Le paramètre de stratégie de groupe **Taille d'invité verrouillée** d'Horizon Client est prioritaire sur la personnalisation de la résolution d'affichage. Pour plus d'informations, reportez-vous à la section Paramètres de définition de scripts des objets de stratégie de groupe (GPO) des clients.

Procédure

1. Démarrez Horizon Client et connectez-vous à un serveur.
2. Dans la fenêtre de sélection des postes de travail et des applications, cliquez avec le bouton droit sur le poste de travail distant, puis sélectionnez **Paramètres**.
3. Dans le menu **Se connecter via**, sélectionnez **VMware Blast** ou **PCoIP**.
4. Dans le menu déroulant **Affichage**, sélectionnez **Plein écran**, **Fenêtre - Grande**, **Fenêtre - Petite** ou **Personnalisé**.
5. Pour personnaliser la résolution d'affichage, sélectionnez-en une dans le menu déroulant **Résolution**.

   Si vous sélectionnez **Automatique** (paramètre par défaut), Horizon Client ajuste le poste de travail distant à la taille de la fenêtre du client. Si le poste de travail distant ne prend pas en charge la résolution d'affichage que vous sélectionnez, il utilise le paramètre par défaut.

6 Pour personnaliser la mise à l'échelle de l'affichage, sélectionnez une taille de mise à l'échelle dans le menu déroulant **Mise à l'échelle**.

   Si vous sélectionnez **Automatique** (paramètre par défaut), Horizon Client synchronise la mise à l'échelle de l'affichage du système client avec le poste de travail distant.

7 Cliquez sur **OK** pour enregistrer les modifications.

Utiliser des périphériques USB

Avec la fonctionnalité de redirection USB, vous pouvez utiliser des périphériques USB connectés localement, tels que des lecteurs USB, dans un poste de travail distant ou une application publiée.

Lorsque vous utilisez la fonctionnalité de redirection USB, la plupart des périphériques USB connectés au système client local deviennent accessibles depuis les menus de Horizon Client. Vous pouvez connecter et déconnecter les périphériques à partir de ces menus.

Pour plus d'informations sur la configuration requise des périphériques USB et les limitations de la redirection USB, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Pour connecter des périphériques USB à un poste de travail distant ou à une application publiée, vous pouvez utiliser un processus manuel ou automatique.

Cette procédure explique comment utiliser Horizon Client pour configurer la connexion automatique de périphériques USB à un poste de travail distant ou à une application publiée. Vous pouvez également configurer la connexion automatique en utilisant l'interface de ligne de commande Horizon Client ou en créant une stratégie de groupe.

Pour plus d'informations sur l'interface de ligne de commande, consultez Exécution d'Horizon Client depuis la ligne de commande. Pour plus d'informations sur la configuration des stratégies de groupe, consultez le document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Conditions préalables

- Pour pouvoir utiliser des périphériques USB avec un poste de travail distant ou une application publiée, il faut qu'un administrateur Horizon active la fonctionnalité de redirection USB.

  Cette tâche inclut l'installation du composant de redirection USB d'Horizon Agentet peut inclure la configuration de stratégies concernant la redirection USB. Pour plus d'informations, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon* et à la section Paramètres USB des objets de stratégie de groupe (GPO) des clients.

- Le composant de redirection USB doit être installé dans Horizon Client. Si vous n'avez pas inclus ce composant dans l'installation, désinstallez Horizon Client, puis exécutez de nouveau le programme d'installation pour inclure le composant de redirection USB.

Pour les instructions d'installation, reportez-vous au document *Guide d'installation et de configuration de VMware Horizon Client pour Windows*.

- Familiarisez-vous avec Limitations de la redirection USB.

Procédure

- Connectez manuellement le périphérique USB à un poste de travail distant.
  a Connectez le périphérique USB au système client local.
  b Dans la barre de menus VMware Horizon Client du poste de travail distant, cliquez sur **Connecter un périphérique USB**.
  c Sélectionnez un périphérique USB.

  Le périphérique est redirigé manuellement du système local vers le poste de travail distant.
- Connectez le périphérique USB à une application publiée.
  a Connectez le périphérique USB au système client local.
  b Démarrez Horizon Client et connectez-vous à l'application publiée.
  c Cliquez sur l'icône **Paramètres** (engrenage) dans le coin supérieur droit de la fenêtre de sélection des postes de travail et applications et cliquez sur **Périphériques USB**.
  d Dans le volet de droite, sélectionnez le périphérique USB, cliquez sur **Connecter**, sélectionnez l'application publiée et cliquez sur **OK**.

  Horizon Client connecte le périphérique USB à l'application publiée que vous avez sélectionnée. Le périphérique USB est également accessible aux applications qui se trouvent dans la même batterie que l'application que vous avez sélectionnée.
  e (Facultatif) Pour configurer Horizon Client pour qu'il connecte automatiquement le périphérique USB à l'application publiée lorsqu'elle est lancée, sélectionnez la case à cocher **Se connecter automatiquement au démarrage**.
  f (Facultatif) Pour configurer Horizon Client pour qu'il connecte automatiquement le périphérique USB à l'application publiée lorsque vous branchez le périphérique sur le système local, sélectionnez la case à cocher **Se connecter automatiquement lors de l'insertion**.

  L'application publiée doit être activée et doit être au premier plan pour que ce comportement prenne effet.
  g Pour fermer la boîte de dialogue Paramètres, cliquez sur **OK**.
  h Lorsque vous avez fini d'utiliser l'application publiée, ouvrez la boîte de dialogue Paramètres, sélectionnez **Périphériques USB**, puis **Déconnecter**.

  Vous devez libérer le périphérique USB pour pouvoir y accéder depuis votre système local.

- Configurez Horizon Client de manière à connecter automatiquement des périphériques USB à un poste de travail distant lorsque vous les branchez au système local.

  Utilisez la fonction de connexion automatique si vous prévoyez de connecter des périphériques qui utilisent des pilotes MTP, tels que les smartphones et tablettes Samsung fonctionnant sous Android.

  a Avant de brancher le périphérique USB, démarrez Horizon Client et connectez-vous au poste de travail distant.

  b Dans la barre de menus VMware Horizon Client du poste de travail distant, sélectionnez **Connecter le périphérique USB > Se connecter automatiquement à l'insertion**.

  c Branchez le périphérique USB.

  Les périphériques USB que vous connectez à votre système local après le démarrage d'Horizon Client sont redirigés vers le poste de travail distant.

- Configurez Horizon Client de manière à connecter automatiquement des périphériques USB à un poste de travail distant au démarrage d'Horizon Client.

  a Dans la barre de menus VMware Horizon Client du poste de travail distant, sélectionnez **Connecter le périphérique USB > Se connecter automatiquement à l'insertion**.

  b Branchez le périphérique USB et redémarrez Horizon Client.

  Les périphériques USB connectés au système local au démarrage de Horizon Client sont redirigés vers le poste de travail distant.

Résultats

Le périphérique USB apparaît dans le poste de travail distant ou l'application publiée. Un périphérique USB peut prendre jusqu'à 20 secondes pour s'afficher sur le poste de travail distant ou dans l'application publiée. Lorsque vous connectez le périphérique à un poste de travail pour la première fois, il peut vous être demandé d'installer des pilotes.

Si le périphérique USB n'apparaît pas sur le poste de travail distant ou l'application publiée après plusieurs minutes, déconnectez, puis reconnectez le périphérique à l'ordinateur client.

Étape suivante

Si vous rencontrez des problèmes avec la redirection USB, consultez la rubrique sur la résolution de problèmes de redirection USB dans le document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Limitations de la redirection USB

La fonction de redirection USB comporte des limitations.

- Lorsque vous accédez à un périphérique USB à partir d'un menu d'Horizon Client et que vous utilisez le périphérique dans un poste de travail distant ou l'application publiée, vous ne pouvez pas accéder au périphérique USB sur le périphérique local.

- Les périphériques USB qui ne sont pas affichés dans le menu, mais qui sont disponibles dans un poste de travail distant ou une application publiée, incluent des périphériques d'interface humaine, tels que des claviers et des dispositifs de pointage. Le poste de travail distant ou l'application publiée et l'ordinateur local utilisent ces périphériques en même temps. L'interaction avec ces périphériques USB peut parfois être lente à cause de la latence du réseau.
- Des lecteurs de disques USB de taille importante peuvent nécessiter plusieurs minutes avant d'apparaître sur le poste de travail distant ou l'application publiée.
- Certains périphériques USB requièrent des pilotes spécifiques. Si un pilote requis n'est pas déjà installé sur un poste de travail distant, vous pouvez être invité à l'installer lorsque vous connectez le périphérique USB au poste de travail distant ou à l'application publiée.
- Si vous prévoyez d'attacher des périphériques USB qui utilisent des pilotes MTP, tels que des smartphones et des tablettes Samsung fonctionnant sous Android, configurez Horizon Client afin qu'il connecte automatiquement les périphériques USB au poste de travail distant ou à l'application publiée. Dans le cas contraire, si vous tentez de rediriger manuellement le périphérique USB à l'aide d'un élément de menu, le périphérique n'est pas redirigé, sauf si vous le débranchez avant de le brancher de nouveau.
- Ne vous connectez pas à des scanners à l'aide du menu **Connecter un périphérique USB**. Pour utiliser un scanner physique, utilisez la fonctionnalité de redirection de scanner. Reportez-vous à la section Utilisation de scanners.
- La redirection de périphériques audio USB dépend de l'état du réseau et n'est pas fiable. Certains périphériques requièrent un débit de données élevé même lorsqu'ils sont inactifs. Les périphériques d'entrée et de sortie audio fonctionnent bien avec la fonctionnalité Audio/Vidéo en temps réel. Vous n'avez pas besoin d'utiliser la redirection USB pour ces périphériques.
- Vous ne pouvez pas formater un lecteur USB redirigé sur un poste de travail publié si vous ne vous connectez pas comme administrateur.
- Une application publiée se connecte automatiquement au démarrage et lorsque les dispositifs insérés ne fonctionnent pas avec les droits d'accès globaux des applications.
- La fonctionnalité de redirection USB ne prend pas en charge les contrôleurs USB non PCI dans le système client, tels que le contrôleur Fresco Logic F-One. Si vous utilisez ce type de contrôleur dans le système client, la redirection USB peut échouer pour tous les périphériques USB du système client.

Note Ne redirigez pas de périphériques USB, tels que les périphériques Ethernet USB et les périphériques à écran tactile, vers un poste de travail distant ou une application publiée. Si vous redirigez un périphérique Ethernet USB, votre système client perd la connectivité réseau. Si vous redirigez un périphérique à écran tactile, le poste de travail distant ou l'application publiée reçoit une entrée tactile, mais pas une entrée de clavier. Si vous avez défini le poste de travail distant ou l'application publiée de manière qu'il ou elle se connecte automatiquement aux périphériques USB, vous pouvez configurer une stratégie afin d'exclure des périphériques spécifiques.

Utilisation de webcams et de microphones

La fonctionnalité Audio/vidéo en temps réel vous permet d'utiliser une webcam ou un microphone du système client local sur un poste de travail distant ou une application publiée. La fonctionnalité Audio/vidéo en temps réel est compatible avec les applications de conférence standard et les applications vidéo basées sur navigateur. Elle prend en charge les webcams standards, les périphériques audio USB et l'entrée audio analogique.

Pour plus d'informations sur la configuration de la fonctionnalité Audio/Vidéo en temps réel sur la machine agent, y compris la configuration de la fréquence d'image et la résolution d'image, consultez le document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Lorsque vous pouvez utiliser une webcam avec la fonctionnalité Audio/Vidéo en temps réel

Si un administrateur Horizon a configuré la fonctionnalité Audio/Vidéo en temps réel, vous pouvez utiliser une webcam intégrée ou connectée à l'ordinateur client dans un poste de travail distant ou une application publiée. Vous pouvez utiliser la webcam dans les applications de conférences telles que Skype, Webex ou Google Hangouts.

Lors de l'installation d'une application telle que Skype, Webex ou Google Hangouts sur un poste de travail distant, vous pouvez sélectionner des périphériques d'entrée et de sortie dans les menus de l'application.

Pour les postes de travail virtuels sur lesquels Horizon Agent 7.9 ou version antérieure est installé, et pour les postes de travail et les applications publiés, Audio/Vidéo en temps réel ne peut rediriger qu'une seule webcam nommée Webcam virtuelle VMware dans les applications. Pour les postes de travail virtuels sur lesquels Horizon Agent 7.10 ou version ultérieure est installé, Audio/Vidéo en temps réel peut rediriger plusieurs webcams. Le nom de la webcam dirigée est le nom du périphérique réel avec (VDI) ajouté, par exemple Webcam FHD C670i (VDI).

Pour de nombreuses applications, vous n'avez pas à sélectionner un périphérique d'entrée.

Lorsque l'ordinateur client utilise la webcam, la session à distance ne peut pas l'utiliser en même temps. En outre, lorsque la session à distance utilise la webcam, l'ordinateur client ne peut pas l'utiliser en même temps.

Important Si vous utilisez une webcam USB, ne la connectez pas via le menu **Connecter un périphérique USB** d'Horizon Client. Cette opération achemine le périphérique via la redirection USB et les performances ne permettent pas de l'utiliser pour une conversation vidéo.

Si plusieurs webcams sont connectées à l'ordinateur client, vous devez configurer une webcam préférée à utiliser dans les sessions à distance pour les postes de travail et les applications publiés, et pour les postes de travail virtuels qui ne prennent pas en charge plusieurs webcams.

Pour plus d'informations, consultez le document Sélectionner une webcam ou un microphone préféré sur un système client Windows.

Sélectionner une webcam ou un microphone préféré sur un système client Windows

Avec la fonctionnalité audio/vidéo en temps réel, si plusieurs webcams ou microphones sont connectés au système client, vous pouvez spécifier la webcam ou le microphone préféré en configurant des paramètres audio/vidéo en temps réel dans Horizon Client.

Avec la fonctionnalité Audio/Vidéo en temps réel, les périphériques vidéo, les périphériques d'entrée audio et les périphériques de sortie audio fonctionnent sans qu'il soit nécessaire d'utiliser la redirection USB, et la bande passante réseau nécessaire est considérablement réduite. Les périphériques d'entrée audio analogique sont également pris en charge.

Si il ou elle est disponible, la webcam ou le microphone préféré(e) est utilisé(e) sur le poste de travail distant ou l'application publiée. Si la webcam ou le microphone préféré(e) n'est pas disponible, une autre webcam ou un autre microphone est utilisé(e).

Note Si vous utilisez une webcam ou un microphone USB, ne le connectez pas via le menu **Connecter un périphérique USB** d'Horizon Client. En effet, cette opération achemine le périphérique via la redirection USB, si bien qu'il ne pourra pas utiliser la fonctionnalité Audio/Vidéo en temps réel.

Pour les postes de travail virtuels sur lesquels Horizon Agent 7.10 ou version ultérieure est installé, la fonctionnalité audio/vidéo en temps réel prend en charge plusieurs webcams et périphériques de microphone.

Conditions préalables

- Assurez-vous qu'une webcam USB ou un microphone USB ou d'un autre type est installé et opérationnel sur le système client.
- Vérifiez que vous utilisez le protocole d'affichage VMware Blast ou PCoIP pour l'application publiée ou le poste de travail distant.
- Connectez-vous à un serveur.

Procédure

1. Ouvrez la boîte de dialogue **Paramètres** et sélectionnez **Audio/Vidéo en temps réel** dans le volet de gauche.
   - Cliquez sur l'icône **Paramètres** (engrenage) dans le coin supérieur droit de la fenêtre de sélection des postes de travail et applications.
   - Cliquez avec le bouton droit sur un poste de travail distant ou sur une application publiée de la fenêtre de sélection des postes de travail et des applications et sélectionnez **Paramètres**.
2. Pour configurer une webcam préférée, sélectionnez une webcam dans le menu déroulant **Webcam préférée**.

3 Pour configurer un microphone préféré, sélectionnez un microphone spécifique ou **Tous** dans le menu déroulant **Microphone préféré**.

   Si le poste de travail distant prend en charge plusieurs périphériques avec la fonctionnalité audio/vidéo en temps réel et que vous sélectionnez un microphone spécifique, seuls les périphériques du microphone et de la webcam sélectionnés sont redirigés vers le poste de travail distant. Si vous sélectionnez **Tous**, tous les périphériques du microphone et de la webcam disponibles sont redirigés vers le poste de travail distant.

4 Pour enregistrer vos modifications, cliquez sur **OK** ou sur **Appliquer**.

Utilisation de plusieurs périphériques avec la fonctionnalité audio/vidéo en temps réel

Si plusieurs webcams ou microphones sont connectés à l'ordinateur client et que le poste de travail distant prend en charge la redirection de périphériques multiples avec la fonctionnalité audio/vidéo en temps réel, vous pouvez utiliser toutes les webcams et tous les microphones connectés à l'ordinateur client dans le poste de travail distant.

Cette fonctionnalité est prise en charge uniquement avec des postes de travail virtuels sur lesquels Horizon Agent 7.10 ou version ultérieure est installé. Elle n'est pas prise en charge avec les applications publiées ou les postes de travail publiés. Pour plus d'informations sur les exigences système, reportez-vous à la section Configuration système requise pour l'Audio/Vidéo en temps réel.

Voici des conseils relatifs à l'utilisation de plusieurs webcams ou microphones avec la fonctionnalité audio/vidéo en temps réel.

- Lorsque vous vous connectez à un poste de travail distant, la fonctionnalité audio/vidéo en temps réel redirige toutes les webcams et tous les microphones actuellement connectés à l'ordinateur client. Le poste de travail distant décide de la webcam et du microphone par défaut. Vous n'avez pas besoin de configurer une webcam ou un microphone préféré dans Horizon Client.
- Si vous souhaitez utiliser le même microphone par défaut dans les applications telles que Skype for Business, vous devez configurer un microphone par défaut. Dans le cas contraire, tous les microphones sont redirigés et vous devrez sélectionner un microphone à chaque fois que vous utilisez l'application. Pour plus d'informations, reportez-vous à la section Sélectionner une webcam ou un microphone préféré sur un système client Windows.
- Si vous déconnectez une webcam ou un microphone de l'ordinateur client et que ce dernier n'est pas utilisé dans une application du poste de travail distant, la fonctionnalité audio/vidéo en temps réel supprime immédiatement le périphérique dans le poste de travail distant. Si le périphérique est utilisé par une application dans le poste de travail distant, la fonctionnalité audio/vidéo en temps réel supprime le périphérique une fois que l'application l'a publié.
- Le nom d'affichage d'un périphérique redirigé est le nom du périphérique réel, mais avec (VDI) ajouté, par exemple, C670i FHD Webcam (VDI).

- Vous pouvez utiliser plusieurs périphériques redirigés simultanément dans un poste de travail distant.

Sélectionner un haut-parleur préféré pour un poste de travail distant

Si plusieurs haut-parleurs sont connectés au système client, vous pouvez spécifier le haut-parleur préféré pour un poste de travail distant.

Cette fonction présente les limites suivantes :

- Cette fonctionnalité est prise en charge uniquement avec les postes de travail virtuels. Elle n'est pas prise en charge avec les applications publiées et les postes de travail publiés.
- Si vous ajoutez ou supprimez un haut-parleur du système client au cours d'une session distante, les modifications ne prennent pas effet sur le poste de travail distant.

Conditions préalables

- Vérifiez que plusieurs haut-parleurs sont installés et opérationnels sur le système client.
- Vérifiez que vous utilisez le protocole d'affichage VMware Blast pour vous connecter au poste de travail distant. Cette fonctionnalité ne fonctionne pas avec les autres protocoles d'affichage.
- Vérifiez que Horizon Agent 2012 ou version ultérieure est installé sur le poste de travail distant. Pour les versions antérieures de Horizon Agent, le son est lu sur le périphérique audio par défaut connecté au système client.
- Connectez-vous au serveur.

Procédure

1. Ouvrez la boîte de dialogue **Paramètres** et sélectionnez **Audio/Vidéo en temps réel** dans le volet de gauche.
   - Cliquez sur l'icône **Paramètres** (engrenage) dans le coin supérieur droit de la fenêtre de sélection des postes de travail et applications.
   - Dans la fenêtre de sélection des postes de travail et des applications, cliquez avec le bouton droit sur le poste de travail distant, puis sélectionnez **Paramètres**.
2. Sélectionnez un haut-parleur dans le menu déroulant **Haut-parleur préféré**.

   Note Cette fonctionnalité est indépendante de la fonctionnalité Audio/Vidéo en temps réel, même si elle apparaît sur la page **Audio/Vidéo en temps réel**.

   Si vous sélectionnez un haut-parleur spécifique, seul le haut-parleur sélectionné est redirigé vers le poste de travail distant. Si vous sélectionnez **Tout**, tous les haut-parleurs disponibles sont redirigés vers le poste de travail distant. Si vous sélectionnez **Par défaut**, le son est lu sur le périphérique audio par défaut connecté au système client.

3 Pour enregistrer vos modifications, cliquez sur **OK** ou sur **Appliquer**.

Partage de sessions de poste de travail distant

Avec la fonctionnalité de collaboration de session, vous pouvez inviter des utilisateurs à rejoindre une session de poste de travail distant existante. Une session de poste de travail distant qui est partagée de cette manière est appelée session de collaboration. L'utilisateur qui partage une session avec un autre utilisateur est appelé le propriétaire de la session et l'utilisateur qui rejoint une session partagée est appelé un collaborateur de session.

Un administrateur Horizon doit activer la fonctionnalité de collaboration de session.

Pour les postes de travail Windows, cette tâche inclut l'activation de la fonctionnalité de collaboration de session au niveau du pool de postes de travail ou de la batterie de serveurs. Elle peut également inclure l'utilisation de stratégies de groupe pour configurer des fonctionnalités de collaboration de session, telles que les méthodes d'invitation disponibles. Pour plus d'informations sur les exigences, reportez-vous à la section Configuration requise pour la fonctionnalité de collaboration de session.

Pour plus d'informations sur l'activation de la fonctionnalité de collaboration de session pour des postes de travail Windows, consultez le document *Configuration des postes de travail virtuels dans Horizon*. Pour plus d'informations sur l'activation de la fonctionnalité de collaboration de session pour une batterie de serveurs, consultez le document *Configuration d'applications et de postes de travail publiés dans Horizon*. Pour plus d'informations sur l'utilisation de paramètres de stratégie de groupe pour configurer la fonctionnalité de collaboration de session, consultez le document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Pour plus d'informations sur l'activation de la fonctionnalité de collaboration de session pour des postes de travail Linux, consultez le document *Configuration des postes de travail Linux dans Horizon*.

Inviter un utilisateur à rejoindre une session de poste de travail distant

Avec la fonctionnalité de collaboration de session, vous pouvez inviter des utilisateurs à rejoindre une session de poste de travail distant en envoyant des invitations de collaboration par e-mail, dans un message instantané (postes de travail distants Windows uniquement) ou en copiant un lien vers le presse-papiers et en transférant le lien aux utilisateurs.

Vous ne pouvez inviter que les utilisateurs qui appartiennent à un domaine que le serveur autorise pour l'authentification. Vous pouvez inviter jusqu'à cinq utilisateurs par défaut. Un administrateur Horizon peut modifier le nombre maximal d'utilisateurs que vous pouvez inviter.

La fonctionnalité de collaboration de session présente les limitations suivantes.

- Si vous disposez de plusieurs moniteurs, seul le principal est affiché pour les collaborateurs de la session.

- Vous devez sélectionner le protocole d'affichage VMware Blast lorsque vous créez une session de poste de travail distant à partager. La fonctionnalité de collaboration de session ne prend pas en charge les sessions PCoIP ou RDP.
- Le codage matériel H.264 n'est pas pris en charge. Si le propriétaire de la session utilise un codage matériel et qu'un collaborateur rejoint la session, les deux passent au codage logiciel.
- La collaboration anonyme n'est pas prise en charge. Les collaborateurs de la session doivent être identifiables via des mécanismes d'authentification pris en charge par Horizon.
- Les collaborateurs de la session doivent avoir installé Horizon Client pour Windows, Mac ou Linux, ou utiliser HTML Access.
- Si un collaborateur de la session dispose d'une version non prise en charge d'Horizon Client, un message d'erreur s'affiche lorsque l'utilisateur clique sur un lien de collaboration.
- Vous ne pouvez pas utiliser la fonctionnalité de collaboration de session pour partager des sessions d'application publiée.

Conditions préalables

- La fonctionnalité de collaboration de session doit être activée et configurée.
- Pour utiliser la méthode d'invitation par e-mail, une application de messagerie doit être installée.
- Pour utiliser la méthode d'invitation par messagerie instantanée pour un poste de travail distant Windows, Skype Entreprise doit être installé et configuré.

Procédure

1. Connectez-vous à un poste de travail distant pour lequel la fonctionnalité de collaboration de session est activée.

   Vous devez utiliser le protocole d'affichage VMware Blast.

2. Dans la barre d'état système du poste de travail distant, cliquez sur l'icône **VMware Horizon Collaboration**, par exemple,  .

   L'icône de collaboration peut être différente selon la version du système d'exploitation.

3. Lorsque la boîte de dialogue VMware Horizon Collaboration s'ouvre, entrez le nom d'utilisateur (par exemple, **`testuser`** ou **`domain\testuser`**) ou l'adresse e-mail de l'utilisateur que vous voulez voir rejoindre la session de poste de travail distant.

   La première fois que vous entrez le nom d'utilisateur ou l'adresse e-mail d'un utilisateur particulier, vous devez cliquer sur **Rechercher « *utilisateur* »**, entrer une virgule (,) ou appuyer sur la touche **Entrée** pour valider l'utilisateur. Pour les postes de travail distants Windows, la fonctionnalité de collaboration de session mémorise l'utilisateur la prochaine fois que vous entrez son nom d'utilisateur ou son adresse e-mail.

4 Sélectionnez une méthode d'invitation.

Toutes les méthodes d'invitation peuvent ne pas être disponibles.

Option	Action
E-mail	Copie l'invitation de collaboration dans le Presse-papiers et ouvre un nouvel e-mail dans l'application de messagerie par défaut. Une application de messagerie doit être installée pour utiliser cette méthode d'invitation.
Messagerie instantanée	(Postes de travail distants Windows uniquement) Copie l'invitation de collaboration dans le Presse-papiers et ouvre une nouvelle fenêtre dans Skype Entreprise. Appuyez sur Ctrl+V pour coller le lien dans la fenêtre Skype Entreprise. Skype Entreprise doit être installé et configuré pour utiliser cette méthode d'invitation.
Copier le lien	Copie l'invitation de collaboration dans le Presse-papiers. Vous devez ouvrir manuellement une autre application, comme le Bloc-notes, et appuyer sur Ctrl+V pour coller l'invitation.

Résultats

Une fois l'invitation envoyée, l'icône VMware Horizon Collaboration s'affiche également sur le poste de travail et l'interface utilisateur de la collaboration de session se transforme en tableau de bord qui indique l'état actuel de la session de collaboration et permet d'exécuter certaines actions.

Lorsqu'un collaborateur de session accepte votre invitation à rejoindre une session de poste de travail distant Windows, la fonctionnalité de collaboration de session vous avertit et un point rouge s'affiche sur l'icône VMware Horizon Collaboration dans la barre d'état système. Lorsqu'un collaborateur de session accepte votre invitation à rejoindre une session de poste de travail distant Linux, une notification s'affiche dans le poste de travail de session principale.

Étape suivante

Gérez la session de poste de travail distant dans la boîte de dialogue VMware Horizon Collaboration. Reportez-vous à la section Gérer une session de poste de travail distant partagée.

Gérer une session de poste de travail distant partagée

Une fois l'invitation de collaboration de session envoyée, l'interface utilisateur de la collaboration de session se transforme en tableau de bord qui indique l'état actuel de la session de poste de travail distant partagée et vous permet d'exécuter certaines actions.

Un administrateur Horizon peut empêcher le transfert de contrôle à un collaborateur de session. Pour les postes distants Windows, reportez-vous au paramètre de stratégie de groupe **Autoriser le contrôle de transmission à des collaborateurs** dans le document *Configuration des fonctionnalités de poste de travail distant dans Horizon*. Pour les postes de travail distants Linux, reportez-vous au paramètre `collaboration.enableControlPassing` du document *Configuration des postes de travail Linux dans Horizon*.

Conditions préalables

Démarrez une session de collaboration. Reportez-vous à la section Inviter un utilisateur à rejoindre une session de poste de travail distant.

Procédure

1 Dans le poste de travail distant, cliquez sur l'icône **VMware Horizon Collaboration** dans la barre d'état système.

Les noms de tous les collaborateurs de session s'affichent dans la colonne Nom et leur état s'affiche dans la colonne État.

2 Utilisez le tableau de bord Collaboration de session VMware Horizon pour gérer la session collaborative.

Option	Action
Révoquer une invitation ou supprimer un collaborateur	Cliquez sur **Supprimer** dans la colonne État.
Rendre le contrôle à un collaborateur de session	Une fois que le collaborateur de session a rejoint la session, basculez le commutateur dans la colonne Contrôle sur **Activé**. Pour reprendre le contrôle de la session, double-cliquez ou appuyez sur n'importe quelle touche. Le collaborateur de session peut également rendre le contrôle en basculant le commutateur dans la colonne Contrôle sur **Désactivé** ou en cliquant sur le bouton **Rendre le contrôle**.
Ajouter un collaborateur	Cliquez sur **Ajouter des collaborateurs**.
Mettre fin à la session de collaboration	Cliquez sur **Mettre fin à la collaboration**. Tous les collaborateurs actifs sont déconnectés. Dans les postes de travail distants Windows, vous pouvez également arrêter la session collaborative en cliquant sur le bouton **Arrêter** en regard de l'icône **Collaboration de session VMware Horizon**. Le bouton **Arrêter** n'est pas disponible dans les postes de travail distants Linux.

Rejoindre une session de poste de travail distant

Avec la fonctionnalité de collaboration de session, vous pouvez cliquer sur le lien dans une invitation de collaboration pour rejoindre une session de poste de travail distant. Le lien peut se trouver dans un e-mail, un message instantané ou dans un document que le propriétaire de la session vous transfère. Vous pouvez également vous connecter au serveur et double-cliquer sur l'icône de la session dans la fenêtre de sélection des applications et des postes de travail distants.

Cette procédure décrit la façon de rejoindre une session de poste de travail distant à partir d'une invitation de collaboration.

Note Dans un environnement Architecture Cloud Pod, vous ne pouvez pas rejoindre une session de collaboration en vous connectant au serveur, sauf si vous vous connectez à l'espace du propriétaire de la session.

Lorsque vous rejoignez une session de poste de travail distant avec la fonctionnalité de collaboration de session, vous ne pouvez pas utiliser les fonctionnalités suivantes dans la session de poste de travail distant.

- Redirection USB
- Audio/Vidéo en temps réel (RTAV)
- Redirection multimédia
- Redirection du lecteur client
- Redirection de carte à puce
- VMware Integrated Printing
- Redirection de Microsoft Lync
- Redirection de fichier et fonctionnalité Conserver dans le Dock
- Redirection du Presse-papiers

Vous ne pouvez pas non plus modifier la résolution du poste de travail distant dans la session de poste de travail distant.

Conditions préalables

Pour rejoindre une session de poste de travail distant avec la fonctionnalité de collaboration de session, Horizon Client pour Windows, Mac ou Linux doit être installé sur le système client, ou vous devez utiliser HTML Access.

Procédure

1. Cliquez sur le lien dans l'invitation de collaboration.

   Horizon Client s'ouvre sur le système client.

2. Entrez vos informations d'identification pour vous connecter à Horizon Client.

   Une fois que vous êtes authentifié, la session de collaboration commence et vous pouvez voir le poste de travail distant du propriétaire de la session. Si le propriétaire de la session vous transfère le contrôle de la souris et du clavier, vous pouvez utiliser le poste de travail distant.

3. Pour rendre le contrôle de la souris et du clavier au propriétaire de la session, cliquez sur l'icône **VMware Horizon Collaboration** dans la barre d'état système et basculez le commutateur dans la colonne Contrôle sur **Désactivé** ou cliquez sur le bouton **Rendre le contrôle**.

4. Pour quitter la session de collaboration, cliquez sur **Options > Se déconnecter**.

Partager des lecteurs et des dossiers locaux

Avec la fonctionnalité de redirection du lecteur client, vous pouvez partager des dossiers et des lecteurs sur le système client local avec des postes de travail distants et des applications publiées.

Les lecteurs partagés peuvent comporter des lecteurs mappés et des périphériques de stockage USB. Les lecteurs mappés peuvent avoir des chemins d'accès UNC (Universal Naming Convention).

La longueur maximale d'un nom de dossier partagé est de 117 caractères.

La fonctionnalité de redirection du lecteur client ne prend pas en charge le partage de Microsoft OneDrive, Google Drive et du stockage de fichiers d'entreprise.

Sur un poste de travail distant Windows, les lecteurs et les dossiers partagés s'affichent dans le dossier **Cet ordinateur** ou dans le dossier **Ordinateur**, selon la version de système d'exploitation Windows. Dans une application publiée, par exemple le bloc-notes, vous pouvez rechercher et ouvrir un fichier situé dans un dossier ou un lecteur partagé.

Les paramètres de redirection du lecteur client s'appliquent à tous les postes de travail distants et à toutes les applications publiées.

Conditions préalables

Pour partager des dossiers et des lecteurs avec un poste de travail distant ou une application publiée, la fonctionnalité de redirection du lecteur client doit être installée dans Horizon Agent. La fonctionnalité de redirection du lecteur client est installée par défaut.

Vous pouvez masquer la fonctionnalité de redirection du lecteur client dans Horizon Client en activant un paramètre de stratégie de groupe. Pour plus d'informations, consultez **Désactiver le partage de fichiers et de dossiers** dans Paramètres généraux des objets de stratégie de groupe (GPO) de clients.

Avec Horizon Agent 7.8 et versions ultérieures, vous pouvez configurer le comportement de la lettre de lecteur pour les lecteurs qui sont redirigés par la fonctionnalité de redirection du lecteur client en configurant le paramètre de stratégie de groupe **Afficher le périphérique redirigé avec la lettre de lecteur**. Pour plus d'informations, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Avec Horizon Agent 7.9 et versions ultérieures, vous pouvez inclure ou exclure des dossiers sur des périphériques pour lesquels des ID de fournisseur et de produit spécifiés sont redirigés à l'aide des paramètres de stratégie de groupe **Inclure un périphérique Vid/Pid** et **Exclure un périphérique Vid/Pid**. Pour plus d'informations, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Avec Horizon Agent 7.10 et version ultérieure, vous pouvez configurer le mode de mappage des lettres de lecteur à l'aide des paramètres de stratégie de groupe **Configurer le mode de mappage de lettre de lecteur** et **Définir la table de mappage de lettre de lecteur**. Pour plus d'informations, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Si le tunnel sécurisé est activé sur l'instance du Serveur de connexion, la configuration du navigateur sur le système client pour utiliser un serveur proxy peut affecter les performances de la redirection du lecteur client. Pour obtenir les meilleures performances de redirection du lecteur client, configurez le navigateur afin qu'il n'utilise pas un serveur proxy ou qu'il détecte automatiquement les paramètres du réseau local.

Procédure

1 Ouvrez la boîte de dialogue Paramètres et affichez le volet Partage.

Option	Description
Depuis la fenêtre de sélection des postes de travail et applications	Cliquez avec le bouton droit sur l'icône d'un poste de travail distant ou d'une application publiée, sélectionnez **Paramètres** et sélectionnez **Partage** dans le volet de gauche de la fenêtre qui s'affiche.
Dans la boîte de dialogue Partage qui s'affiche lors de la connexion à un poste de travail distant ou à une application publiée	Cliquez sur le lien **Paramètres > Partage** de la boîte de dialogue.
Depuis un poste de travail distant	Sélectionnez **Options > Partager les dossiers** dans la barre de menus.

2 Configurez les paramètres de la redirection de lecteur client.

Option	Action
Partager un dossier ou un lecteur spécifique avec des postes de travail distants et des applications publiées	Cliquez sur le bouton **Ajouter**, recherchez et sélectionnez le dossier ou le lecteur à partager, puis cliquez sur **OK**. **Note** Si un périphérique USB est déjà connecté à un poste de travail distant ou à une application publiée avec la fonctionnalité de redirection USB, vous ne pouvez pas partager un dossier sur le périphérique USB. De plus, n'activez pas la fonctionnalité de redirection USB qui connecte automatiquement les périphériques USB au démarrage ou lorsque le périphérique est inséré. Si vous l'activez, au prochain démarrage d'Horizon Client ou lorsque vous branchez le périphérique USB, le périphérique se connecte à l'aide de la fonctionnalité de redirection USB et non pas avec la fonctionnalité de redirection du lecteur client. Si le mappage de lettre de lecteur est configuré, les dossiers configurés dans la liste de partage ne sont pas redirigés. Pour plus d'informations, reportez-vous à la section « Utiliser une stratégie de groupe pour configurer le comportement de la lettre de lecteur » dans le document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.
Arrêter le partage d'un dossier ou d'un lecteur spécifique	Sélectionnez le dossier ou le lecteur dans la liste des dossiers et cliquez sur le bouton **Supprimer**.
Autoriser les postes de travail distants et les applications publiées à accéder à des fichiers de votre répertoire d'utilisateurs local	Cochez la case **Partager vos fichiers locaux *nom-utilisateur***.

Option	Action
Partager des périphériques de stockage USB avec des postes de travail distants et des applications publiées	Cochez la case **Autoriser l'accès au stockage amovible**. La fonctionnalité de redirection du lecteur client partage automatiquement tous les périphériques de stockage USB insérés dans votre système client et tous les lecteurs externes connectés via FireWire et Thunderbolt. Il n'est pas nécessaire de sélectionner un périphérique spécifique à partager. **Note** Les périphériques de stockage USB déjà connectés à un poste de travail distant ou à une application publiée avec la fonctionnalité de redirection USB ne sont pas partagés. Si vous utilisez une clé USB chiffrée, vous devez démarrer Horizon Client avant de brancher le périphérique USB afin qu'Horizon Client puisse le détecter. Si cette case est décochée, vous pouvez utiliser la fonctionnalité de redirection USB pour connecter des périphériques de stockage USB à des postes de travail distants et à des applications publiées.
Ne pas afficher la boîte de dialogue Partage lorsque vous vous connectez à un poste de travail distant ou à une application publiée	Cochez la case **Ne pas afficher la boîte de dialogue lors de la connexion à un poste de travail ou à une application**. Si cette case est cochée, la boîte de dialogue Partage s'affiche la première fois que vous vous connectez à un poste de travail distant ou à une application publiée. Par exemple, si vous ouvrez une session sur un serveur avant de vous connecter à un poste de travail distant, la boîte de dialogue Partage s'ouvre. Si vous vous connectez ensuite à un autre poste de travail distant ou à une autre application publiée, cette boîte de dialogue ne s'ouvre pas. Pour afficher de nouveau cette boîte de dialogue, vous devez vous déconnecter du serveur, puis rouvrir une session.

Étape suivante

Vérifiez que vous pouvez voir les dossiers partagés depuis le poste de travail distant ou l'application publiée.

- Depuis un poste de travail distant Windows, ouvrez l'explorateur de fichiers et effectuez une recherche dans le dossier **Cet ordinateur**, ou ouvrez l'explorateur Windows et effectuez une recherche dans le dossier **Ordinateur**, selon la version de système d'exploitation Windows.
- Depuis une application publiée, sélectionnez **Fichier > Ouvrir** ou **Fichier > Enregistrer sous** et accédez au dossier ou au lecteur.

Les dossiers et les lecteurs que vous avez sélectionnés pour le partage peuvent utiliser une (ou plusieurs) des conventions d'affectation de noms suivantes.

Convention d'affectation de noms	Exemple
nom du dossier sur *nom du poste de travail*	jsmith sur JSMITH-W03
nom du dossier (*numéro du lecteur*:)	jsmith (Z:)
nom du dossier sur *nom du poste de travail* (*numéro du lecteur*:)	jsmith JSMITH-W03 (Z:)

Pour certaines versions d'Horizon Agent, un dossier redirigé peut avoir deux entrées, comme sous **Périphériques et lecteurs** et **Emplacements réseau** dans Windows 10, et les deux entrées peuvent s'afficher en même temps. Si toutes les étiquettes de volume (de A: à Z:) sont déjà utilisées, le dossier redirigé n'a qu'une seule entrée.

Ouvrir les fichiers locaux dans des applications publiées

Vous pouvez activer la fonctionnalité permettant d'ouvrir des fichiers locaux dans des applications publiées, directement depuis le système de fichiers local.

Avec cette fonctionnalité, le menu **Ouvrir avec** sur le système client répertorie les applications publiées disponibles lorsque vous cliquez avec le bouton droit sur un fichier local.

Vous pouvez également définir les fichiers pour qu'ils s'ouvrent automatiquement dans des applications publiées lorsque vous double-cliquez dessus. Avec cette fonctionnalité, tous les fichiers sur le système de fichiers local avec certaines extensions de fichier sont enregistrés avec le serveur sur lequel vous avez ouvert une session. Par exemple, si Microsoft Word est une application publiée disponible sur le serveur, vous pouvez cliquer avec le bouton droit sur un fichier `.docx` dans le système de fichiers local et ouvrir le fichier avec l'application publiée Microsoft Word.

Conditions préalables

Pour ouvrir des fichiers locaux dans des applications publiées, une instance d'Horizon Administrator doit installer la fonctionnalité de redirection du lecteur client dans Horizon Agent. La fonctionnalité de redirection du lecteur client est installée par défaut. Pour plus d'informations, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Vous pouvez masquer la fonctionnalité de redirection du lecteur client dans Horizon Client en activant un paramètre de stratégie de groupe. Pour plus d'informations, consultez **Désactiver le partage de fichiers et de dossiers** dans Paramètres généraux des objets de stratégie de groupe (GPO) de clients.

Procédure

1 Connectez-vous à un serveur.

2 Ouvrez la boîte de dialogue Paramètres et affichez le volet Partage.

Option	Description
Depuis la fenêtre de sélection des postes de travail et applications	Cliquez avec le bouton droit sur l'icône d'un poste de travail distant ou d'une application publiée, sélectionnez **Paramètres** et sélectionnez **Partage** dans le volet de gauche de la fenêtre qui s'affiche.
Dans la boîte de dialogue Partage qui s'affiche lors de la connexion à un poste de travail distant ou à une application publiée	Cliquez sur le lien **Paramètres > Partage** de la boîte de dialogue.
Depuis un poste de travail distant	Sélectionnez **Options > Partager les dossiers** dans la barre de menus.

3 Cochez la case **Ouvrir les fichiers locaux dans des applications hébergées**.

Lorsque cette option est activée, vous pouvez cliquer avec le bouton droit sur un fichier dans le système de fichiers local et choisir d'ouvrir le fichier dans une application publiée. Vous

pouvez également modifier les propriétés du fichier pour que tous les fichiers avec cette extension soient ouverts avec l'application publiée par défaut, comme lorsque vous double-cliquez sur le fichier. Par exemple, vous pouvez cliquer avec le bouton droit sur un fichier, sélectionner **Propriétés** et cliquer sur **Modifier** afin de sélectionner l'application publiée pour ouvrir les fichiers de ce type.

Copier et coller

Par défaut, vous pouvez copier et coller à partir du système client vers un poste de travail distant ou une application publiée.

Si vous utilisez le protocole d'affichage VMware Blast ou PCoIP, un administrateur Horizon peut configurer cette fonctionnalité pour que les opérations Copier et Coller soient autorisées uniquement depuis le système client vers un poste de travail distant ou une application publiée, ou uniquement depuis un poste de travail distant ou une applications publiée vers le système client, les deux ou aucun.

Un administrateur Horizon configure la possibilité de copier et coller en définissant des stratégies de groupe d'agent. Selon la version d'Horizon Server et de l'agent, un administrateur Horizon peut également avoir la possibilité d'utiliser des stratégies de groupe pour limiter les formats de Presse-papiers lors des opérations Copier et Coller, ou d'utiliser des stratégies de carte à puce pour contrôler le comportement de la fonctionnalité Copier-Coller sur les postes de travail distants. Pour plus d'informations, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Copier et coller du texte et des images

Par défaut, vous pouvez copier et coller à partir du système client vers un poste de travail distant ou une application publiée. Vous pouvez également copier et coller à partir d'un poste de travail distant ou d'une application publiée vers le système client, ou entre deux postes de travail distants ou applications publiées, si un administrateur Horizon active ces fonctionnalités.

Les formats de données suivants sont pris en charge.

- CF_BITMAP
- CF_DIB
- CF_HDROP (type de fichier)
- CF_UNICODETEXT
- Biff12
- Art::GVML ClipFormat
- Format HTML
- Format RTF (Rich Text Format)

Par exemple, pour copier du texte sur le système client, sélectionnez le texte et appuyez sur Ctrl+C. Pour coller le texte dans un poste de travail distant, appuyez sur Ctrl+V dans le poste de travail distant.

Cette fonction présente les limites suivantes :

- Si vous copiez du texte formaté, certaines de ces données comprennent du texte et certaines comprennent des informations concernant le formatage. Si vous copiez un volume considérable de texte formaté ou du texte avec une image, il est possible que seule une partie du texte, ou sa totalité, s'affiche, mais sans formatage ou image lorsque vous essayez de le coller. Ce problème se produit, car les trois types de données sont parfois stockés séparément. Par exemple, les images peuvent être stockées en tant qu'images ou en tant que données RTF, selon le type de document.
- Si le texte et les données RTF prennent moins de la taille maximale du Presse-papiers, le texte formaté est collé. Il arrive souvent que les données RTF ne peuvent être tronquées. Ainsi, si le texte et le formatage prennent plus de la taille maximale du Presse-papiers, les données RTF sont ignorées et le texte brut est collé.
- Si vous ne parvenez pas à coller l'ensemble du texte formaté et les images que vous avez sélectionnées en une seule fois, effectuez l'opération en plusieurs fois en copiant et collant de plus petits volumes.

Copier et coller des fichiers et des dossiers

Par défaut, vous pouvez copier et coller des fichiers et des dossiers à partir de votre système client vers un poste de travail distant ou une application publiée. Vous pouvez également copier et coller des fichiers et des dossiers à partir d'un poste de travail distant ou d'une application publiée vers le système client si un administrateur Horizon active ces fonctionnalités.

Par exemple, pour copier un fichier depuis le système client, sélectionnez-le et appuyez sur Ctrl+C. Pour coller le fichier sur un poste de travail distant, appuyez sur Ctrl+V sur le poste de travail distant.

Cette fonctionnalité requiert Horizon Agent 2012 ou version ultérieure sur la machine agent.

Pour utiliser cette fonctionnalité, la fonctionnalité de redirection du lecteur client doit être installée sur la machine agent. Pour plus d'informations, reportez-vous au document *Configuration des postes de travail virtuels dans Horizon* ou *Configuration d'applications et de postes de travail publiés dans Horizon*.

Vous pouvez désactiver cette fonctionnalité en activant les paramètres **Filtrer les fichiers et les dossiers des données de Presse-papiers entrantes** et **Filtrer les fichiers et les dossiers des données de Presse-papiers sortantes** dans le paramètre de stratégie de groupe **Configurer les formats de redirection du Presse-papiers** pour la machine agent. Pour plus d'informations sur les paramètres de stratégie de groupe de l'agent qui contrôlent cette fonctionnalité, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Cette fonction présente les limites suivantes :

- Lorsque vous essayez de copier et coller plusieurs fichiers, elle peut ne pas fonctionner pour certains dossiers spéciaux, tels que le dossier de poste de travail ou un dossier de liste de fichiers récemment accédés, car ces dossiers peuvent afficher des fichiers et des dossiers qui ne se trouvent pas dans le même dossier parent. Cette fonctionnalité peut uniquement copier et coller des fichiers et des dossiers qui se trouvent dans le même dossier parent.
- Elle peut ne pas fonctionner pour certaines applications, telles que WordPad et PowerPoint.

Journalisation des activités copier et coller

Lorsque vous activez la fonctionnalité d'audit du Presse-papiers, Horizon Agent enregistre des informations sur les activités copier et coller dans un journal des événements sur la machine agent. La fonctionnalité d'audit du Presse-papiers est désactivée par défaut.

Cette fonctionnalité s'applique uniquement au copier-coller du texte et des images. Elle ne s'applique pas au copier-coller des fichiers et des dossiers.

Pour activer la fonctionnalité d'audit du Presse-papiers, vous devez configurer le paramètre de stratégie de groupe **Configurer l'audit du Presse-papiers**.

Si Horizon Agent 7.6 est installé sur la machine agent, seules les informations sur les données de Presse-papiers copiées de la machine agent sur la machine cliente sont enregistrées dans le journal des événements. Si Horizon Agent 7.7 ou version ultérieure est installé sur la machine agent, vous pouvez configurer la fonctionnalité d'audit du Presse-papiers pour enregistrer des informations uniquement sur les données copiées de la machine cliente sur la machine agent, uniquement sur les données copiées de la machine agent sur la machine cliente, ou sur les données copiées dans les deux sens.

Vous pouvez éventuellement configurer le paramètre de stratégie de groupe **Bloquer la redirection du Presse-papiers du côté client lorsque le client ne prend pas en charge l'audit** pour indiquez si vous voulez bloquer la redirection du Presse-papiers vers les clients qui ne prennent pas en charge la fonctionnalité d'audit du Presse-papiers.

Pour plus d'informations sur les paramètres de stratégie de groupe pour la redirection du Presse-papiers, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Le journal des événements dans lequel sont enregistrées les informations sur les activités copier et coller se nomme VMware Horizon RX Audit. Pour afficher le journal des événements sur la machine agent, utilisez l'Observateur d'événements de Windows. Pour afficher le journal des événements dans un emplacement centralisé, configurez VMware Log Insight ou le Collecteur d'événements de Windows. Pour plus d'informations sur Log Insight, rendez-vous sur https://docs.vmware.com/fr/vRealize-Log-Insight/index.html. Pour plus d'informations sur le Collecteur d'événements Windows, reportez-vous à la documentation de Microsoft.

Configuration de la taille de la mémoire du Presse-papiers du client

La taille de la mémoire du Presse-papiers est configurable pour le serveur et le client.

Cette fonctionnalité s'applique uniquement au copier-coller du texte et des images. Elle ne s'applique pas au copier-coller des fichiers et des dossiers.

Lorsqu'une session PCoIP ou VMware Blast est établie, le serveur envoie la taille de la mémoire de son Presse-papiers au client. La taille de mémoire effective du Presse-papiers est la plus petite des valeurs de taille de mémoire du Presse-papiers du serveur et du client.

Pour définir la taille de la mémoire du Presse-papiers du client, modifiez la valeur du registre Windows `HKLM\Software\VMware, Inc.\VMware VDPService\Plugins\MKSVchan\ClientClipboardSize`. Le type de valeur est REG_DWORD. La valeur est spécifiée en Ko. Si vous spécifiez 0 ou si vous ne spécifiez aucune valeur, la taille par défaut de la mémoire du Presse-papiers du client est de 8192 Ko (8 Mo).

En fonction de votre réseau, une taille importante de la mémoire du Presse-papiers peut avoir une incidence négative sur les performances. VMware recommande de ne pas définir la taille de la mémoire du Presse-papiers à une valeur supérieure à 16 Mo.

La taille maximale de la mémoire du Presse-papiers pour les opérations de copier-coller est de 65 535 Ko. Comme cette limite inclut les métadonnées et les données de formatage, la taille réelle des données doit être légèrement inférieure à 65 535 Ko. Pour transférer des quantités de données plus grandes, utilisez la fonctionnalité de redirection du lecteur client.

Glisser-déposer

Le glisser-déposer fonctionne différemment selon la version d'Horizon Agent et la manière dont il est configuré.

Avec Horizon Agent 7.9 et versions ultérieures, vous pouvez glisser-déposer des fichiers, des dossiers, du texte, du texte enrichi et des images entre le système client et des postes de travail distants et des applications publiées. Avec Horizon Agent 7.7 et 7.8, vous ne pouvez glisser-déposer que des fichiers et des dossiers entre le système client et des postes de travail distants et des applications publiées. Les versions antérieures d'Horizon Agent ne prennent pas en charge le glisser-déposer.

Selon la version d'Horizon Agent, un administrateur Horizon peut utiliser certains paramètres de stratégie de groupe ou stratégies de carte à puce pour configurer le comportement du glisser-déposer. Pour obtenir des informations complètes sur la configuration de la fonctionnalité de glisser-déposer, consultez le document *Configuration des fonctionnalités de poste de travail distant dans Horizon* pour votre version de VMware Horizon.

Faire glisser du texte et des images

Avec Horizon Agent 7.9 et versions ultérieures, vous pouvez faire glisser du texte, des images et d'autres formats de données depuis le système client vers une application ouverte dans un poste de travail distant ou une application publiée. Par exemple, vous pouvez faire glisser du texte à partir d'un navigateur sur le système client et le déposer dans l'application WordPad d'un poste de travail distant. Selon la configuration de la fonctionnalité de glisser-déposer, vous pouvez également faire glisser du texte, des images et d'autres formats de données à partir

d'une application ouverte dans un poste de travail distant ou une application publiée vers le système client.

Les formats de données suivants sont pris en charge.

- Format HTML
- Format RTF (Rich Text Format)
- CF_BITMAP
- CF_DIB
- CF_UNICODETEXT
- FileGroupDescriptorW
- FileGroupDescriptor
- FileContents

Un administrateur Horizon peut configurer le comportement du glisser-déposer en configurant des paramètres de stratégie de groupe. Avec Horizon Agent 7.9 et Dynamic Environment Manager 9.8 et versions ultérieures, un administrateur Horizon peut également utiliser des stratégies de carte à puce pour configurer le comportement du glisser-déposer, y compris la désactivation de l'intégralité de la fonctionnalité de glisser-déposer. Pour plus d'informations, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Glisser des fichiers et des dossiers

Avec Horizon Agent 7.7 et versions ultérieures, vous pouvez glisser-déposer des fichiers et des dossiers entre le système client Windows et des postes de travail distants et des applications publiées. Vous pouvez glisser-déposer plusieurs fichiers et dossiers en même temps. Une barre de progression affiche l'état de l'opération de glisser-déposer.

Si vous glissez un fichier ou un dossier entre le système client et un poste de travail distant, le fichier ou le dossier s'affiche dans le système de fichiers sur le système cible. Si vous faites glisser un fichier et le déposer dans une application ouverte, comme le Bloc-notes, le texte s'affiche dans l'application. Si vous faites glisser un fichier dans un nouveau message électronique, le fichier se transforme en pièce jointe dans le message.

Par défaut, le glisser-déposer depuis le système client vers des postes de travail distants et des applications publiées est activé et le glisser-déposer depuis des postes de travail distants et des applications publiées vers le système client est désactivé. Un administrateur Horizon peut contrôler la direction du glisser-déposer en configurant des paramètres de stratégie de groupe.

Le glisser-déposer des fichiers, des dossiers et des contenus de fichier nécessite que la fonctionnalité de redirection du lecteur client soit installée dans Horizon Agent. La fonctionnalité de redirection du lecteur client est installée par défaut. Pour obtenir des informations complètes sur la configuration de la fonctionnalité de glisser-déposer, y compris les exigences de la fonctionnalité, consultez le document *Configuration des fonctionnalités de poste de travail distant dans Horizon* pour votre version de VMware Horizon.

Conseils d'utilisation de la fonctionnalité de glisser-déposer

Lorsque vous utilisez la fonctionnalité de glisser-déposer, suivez ces conseils.

Note Selon la version d'Horizon Agent, il se peut que certains conseils ne s'appliquent pas à votre environnement.

- Vous devez utiliser le protocole d'affichage VMware Blast ou PCoIP.
- Si la fonctionnalité de souris relative est activée (**Options > Activer la souris relative**), vous pouvez glisser-déposer uniquement depuis le système client vers un poste de travail virtuel.
- Lorsqu'une opération de glisser-déposer est en cours, il n'est pas possible d'en démarrer une nouvelle tant que la première opération n'est pas terminée.
- Vous ne pouvez pas utiliser la fonctionnalité de glisser-déposer en mode imbriqué.
- Lors du glisser-déposer, vous devez utiliser le bouton principal de la souris (par défaut le bouton gauche). L'utilisation du bouton secondaire de la souris (par défaut le bouton droit) et l'appui sur Ctrl+Maj+Alt + le bouton principal de la souris ne sont pas pris en charge.
- Vous ne pouvez pas glisser-déposer entre des postes de travail distants.
- Vous ne pouvez pas glisser-déposer entre des applications publiées depuis différentes batteries de serveurs.
- Si vous glissez et déposez un fichier ou un dossier entre le système client et un poste de travail distant, le fichier ou le dossier s'affiche dans le système de fichiers sur le système cible. Si vous faites glisser un fichier et le déposer dans une application ouverte, comme le Bloc-notes, le texte s'affiche dans l'application. Si vous faites glisser un fichier dans un nouveau message électronique, le fichier se transforme en pièce jointe dans le message.
- Vous pouvez glisser-déposer plusieurs fichiers et dossiers en même temps. Une barre de progression affiche l'état de l'opération de glisser-déposer.
- Par défaut, le glisser-déposer depuis le système client vers des postes de travail distants et des applications publiées est activé et le glisser-déposer depuis des postes de travail distants et des applications publiées vers le système client est désactivé.
- Si vous faites glisser du texte formaté, certaines des données comprennent du texte et certaines comprennent des informations sur le formatage. Si vous faites glisser un volume considérable de texte formaté ou du texte avec une image, il est possible que seule une

partie du texte, ou sa totalité, s'affiche, mais sans formatage ou image lorsque vous essayez de le déposer. Ce problème se produit, car les trois types de données sont parfois stockés séparément. Par exemple, les images peuvent être stockées en tant qu'images ou en tant que données RTF, selon le type de document.

- Si vous faites glisser à la fois du texte brut et des données RTF et que la taille totale des données est inférieure au seuil de taille du glisser-déposer, le texte formaté est copié. Comme les données RTF ne peuvent pas être tronquées, si la taille totale des données est supérieure au seuil de taille du glisser-déposer, les données RTF sont ignorées et seul le texte brut (ou une partie du texte brut) est copié.
- Si vous ne parvenez pas à déposer l'ensemble du texte formaté et des images en une seule fois, effectuez l'opération en plusieurs fois en déposant de plus petits volumes.
- Lorsque vous faites glisser un fichier depuis le système client et le déposer dans une application publiée, vous ne pouvez pas cliquer sur **Enregistrer sous** pour copier le fichier sur un autre fichier sur le système client. Vous pouvez cliquer sur **Enregistrer** pour copier le fichier sur le même fichier sur le système client.
- Si vous faites glisser un fichier depuis le système client vers une application dans un poste de travail distant, le fichier est copié sur le poste de travail distant et vous ne pouvez modifier que la copie du fichier.
- Dans une machine Windows 64 bits, si vous ne parvenez pas à faire glisser d'Horizon Client vers une application 64 bits locale, essayez d'utiliser la version 32 bits de l'application locale.
- Si l'application locale cible ne parvient pas à accepter l'objet glissé, essayez de faire glisser l'objet vers le système de fichiers local, puis de le faire glisser vers l'application locale cible à partir du système de fichiers local.
- Un mécanisme de délai d'expiration intégré existe pour la tolérance de panne.

Conseils pour l'utilisation d'applications publiées

Les applications publiées ont l'aspect des applications installées sur le système client local. Lors de l'utilisation des applications publiées, suivez ces conseils.

- Vous pouvez réduire et agrandir une application publiée via l'application publiée. Lorsqu'une application publiée est réduite, elle s'affiche dans la barre des tâches du système client. Vous pouvez également réduire et agrandir l'application publiée en cliquant sur son icône dans la barre des tâches.
- Vous pouvez quitter une application publiée via l'application publiée ou en cliquant avec le bouton droit sur son icône dans la barre des tâches.
- Vous pouvez appuyer sur Alt+Tab pour basculer entre des applications publiées ouvertes.

- Si une application publiée crée un élément de barre d'état système Windows, cet élément s'affiche également dans la barre d'état système du système client. Par défaut, les icônes de la barre d'état système s'affichent uniquement pour afficher les notifications. Vous pouvez personnaliser ce comportement de la même manière que vous personnalisez des applications installées en mode natif.

  Note Si vous ouvrez le Panneau de configuration pour personnaliser les icônes de la zone de notification, les noms des icônes des applications publiées sont répertoriés sous la forme VMware Horizon Client - *application name*.

Se reconnecter aux applications publiées après une déconnexion

Les applications publiées en cours d'exécution peuvent rester ouvertes après la déconnexion d'un serveur dans Horizon Client. Vous pouvez configurer le comportement des applications publiées en cours d'exécution lorsque vous vous reconnectez au serveur dans Horizon Client.

Vous pouvez désactiver les paramètres de comportement de reconnexion des applications publiées dans Horizon Client à partir de la ligne de commande ou en configurant un paramètre de stratégie de groupe. Le paramètre de stratégie de groupe est prioritaire sur le paramètre de ligne de commande. Pour plus d'informations, consultez l'option `-appSessionReconnectionBehavior` dans Utilisation des commandes Horizon Client ou le paramètre de stratégie de groupe **Comportement de reprise d'une session d'application déconnectée** dans Paramètres de définition de scripts des objets de stratégie de groupe (GPO) des clients.

Procédure

1. Dans la fenêtre de sélection des postes de travail et des applications de Horizon Client, cliquez avec le bouton droit sur une application publiée, puis sélectionnez **Paramètres**.
2. Dans le volet Applications distantes qui s'affiche, sélectionnez un paramètre de comportement de reconnexion des applications.

Option	Description
Demander la reconnexion pour ouvrir des applications publiées	Horizon Client vous informe qu'une ou plusieurs applications publiées sont en cours d'exécution lorsque vous vous reconnectez au serveur. Vous pouvez cliquer sur **Se reconnecter aux applications** pour rouvrir les fenêtres des applications publiées ou sur **Pas maintenant** pour ne pas les rouvrir.
Se reconnecter automatiquement pour ouvrir des applications publiées	Les fenêtres des applications en cours d'exécution se rouvrent lorsque vous vous reconnectez au serveur.
Ne pas demander la reconnexion et ne pas se reconnecter automatiquement	Horizon Client ne vous invite pas à rouvrir les applications publiées en cours d'exécution et les fenêtres de celles-ci ne se rouvrent pas lorsque vous vous reconnectez au serveur.

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

Résultats

Le paramètre s'applique la prochaine fois qu'Horizon Client se connecte au serveur.

Utiliser plusieurs sessions d'une application publiée à partir de périphériques clients différents

Lorsque le mode de sessions·multiples est activé pour une application publiée, vous pouvez utiliser plusieurs sessions de la même application publiée lorsque vous vous connectez au serveur depuis différents périphériques clients.

Par exemple, si vous ouvrez une application publiée en mode de sessions·multiples sur le client A, puis que vous ouvrez la même application publiée sur le client B, elle reste ouverte sur le client A et une nouvelle session de l'application publiée s'ouvre sur le client B. En comparaison, lorsque le mode de sessions·multiples est désactivé (mode de session unique), la session de l'application publiée sur le client A se déconnecte et se reconnecte sur le client B.

La fonctionnalité de mode de sessions multiples présente les limites suivantes.

- Le mode de sessions multiples ne fonctionne pas pour les applications qui ne prennent pas en charge plusieurs instances, telles que Skype Entreprise.
- Si la session d'application est déconnectée lorsque vous utilisez une application publiée en mode de sessions multiples, vous êtes déconnecté automatiquement et les données non enregistrées sont perdues.

Conditions préalables

Un administrateur Horizon doit activer le mode de sessions multiples pour le pool d'applications. Les utilisateurs ne peuvent pas modifier le mode de sessions multiples pour une application publiée, sauf si un administrateur Horizon l'autorise. Reportez-vous à *Configuration d'applications et de postes de travail publiés dans Horizon*. Cette fonctionnalité requiert Horizon 7 7.7 ou version ultérieure.

Procédure

1. Connectez-vous à un serveur.
2. Ouvrez la boîte de dialogue Paramètres et sélectionnez **Lancements multiples** dans le volet de gauche.
   - Cliquez sur l'icône **Paramètres** (engrenage) dans le coin supérieur droit de la fenêtre de sélection des postes de travail et applications.
   - Cliquez avec le bouton droit sur un poste de travail distant ou sur une application publiée de la fenêtre de sélection des postes de travail et applications et sélectionnez **Paramètres**.

   Si aucune application publiée n'est disponible pour une utilisation en mode de sessions multiples, le paramètre **Lancements multiples** n'apparaît pas.

3 Sélectionnez les applications publiées que vous voulez utiliser en mode de sessions multiples et cliquez sur **OK**.

Si un administrateur Horizon a appliqué le mode de sessions multiples pour une application publiée, vous ne pouvez pas modifier ce paramètre.

Utiliser un IME (éditeur de méthode d'entrée) local avec des applications publiées

Si vous utilisez des claviers et des paramètres régionaux non anglais, vous pouvez utiliser un éditeur IME (éditeur de méthode d'entrée) installé sur le système client local pour envoyer des caractères non anglais à une application publiée.

Vous pouvez utiliser les touches de raccourci et les icônes de la zone de notification (barre d'état système) du système local pour changer d'IME. Vous n'avez pas besoin d'installer un IME sur le serveur qui héberge l'application publiée.

Lorsque cette fonctionnalité est activée, l'éditeur IME local est utilisé. Si un IME est installé et configuré sur le serveur qui héberge l'application publiée, cet IME distant est ignoré.

Cette fonctionnalité est désactivée par défaut. Lorsque vous activez ou désactivez cette fonctionnalité, vous devez vous déconnecter du serveur et vous reconnecter pour que la modification s'applique.

Conditions préalables

- Vérifiez qu'au moins un IME est installé sur le système client.
- Assurez-vous que la langue d'entrée sur le système client local correspond à la langue utilisée dans l'IME.

Procédure

1 Dans la fenêtre de sélection des postes de travail et applications d'Horizon Client, cliquez avec le bouton droit sur une application publiée, puis sélectionnez **Paramètres**.

2 Dans le volet des applications distantes, cochez la case **Étendre l'IME local aux applications hébergées** et cliquez sur **OK**.

3 Redémarrez la session.

Option	Action
Se déconnecter du serveur	Déconnectez-vous du serveur, reconnectez-vous et reconnectez-vous à l'application publiée. Vous pouvez reprendre les applications publiées déconnectées mais pas fermées, et les postes de travail distants.
Réinitialiser les applications	Cliquez avec le bouton droit sur une icône de l'application publiée, sélectionnez **Paramètres** et cliquez sur **Réinitialiser**. Lorsque vous utilisez cette option, aucun poste de travail distant ouvert n'est déconnecté, mais toutes les applications publiées sont fermées et doivent être redémarrées.

Le paramètre prend effet uniquement après le redémarrage de la session. Le paramètre s'applique à toutes les applications publiées sur le serveur.

4 Utilisez l'éditeur IME local comme vous le faites avec les applications installées localement.

Résultats

La langue et une icône correspondant à l'éditeur IME s'affichent dans la zone de notification (barre d'état système) du système client local. Vous pouvez utiliser des touches de raccourci pour changer de langue ou d'IME. Les combinaisons de touches qui permettent d'accomplir certaines actions (comme Ctrl+X pour couper le texte et Alt+Flèche droite pour passer d'un onglet à un autre) fonctionnent.

Note Sur les systèmes Windows 7 et 8.x, vous pouvez spécifier des touches de raccourci pour les éditeurs IME en utilisant la boîte de dialogue **Services de texte et langues d'entrée** (disponible dans le **Panneau de configuration > Région et langue > onglet Claviers et langues > bouton Modifier les claviers > Services de texte et langues d'entrée > onglet Paramètres de touches avancés**).

Impression à partir d'un poste de travail distant ou d'une application publiée

La fonctionnalité VMware Integrated Printing vous permet d'imprimer sur une imprimante réseau ou une imprimante connectée localement à partir d'un poste de travail distant ou d'une application publiée.

Pour plus d'informations sur l'installation de la fonctionnalité VMware Integrated Printing, reportez-vous au document *Configuration des postes de travail virtuels dans Horizon* ou *Configuration d'applications et de postes de travail publiés dans Horizon*.

Pour plus d'informations sur la configuration de la fonctionnalité VMware Integrated Printing, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Pour plus d'informations sur les types de postes de travail distants qui prennent en charge la fonctionnalité VMware Integrated Printing, reportez-vous à la section Prise en charge des fonctionnalités pour les clients Windows.

Définir les préférences d'impression de la fonctionnalité de VMware Integrated Printing

Vous pouvez définir des préférences d'impression dans un poste de travail distant pour la fonctionnalité de VMware Integrated Printing. Avec la fonctionnalité de VMware Integrated Printing, vous pouvez utiliser des imprimantes locales ou réseau depuis un poste de travail distant Windows sans avoir à installer d'autres pilotes d'imprimante dans celui-ci. Pour chaque imprimante disponible via cette fonction, vous pouvez définir des préférences pour la compression des données, la qualité d'impression, l'impression recto verso, la couleur et d'autres paramètres.

Dans un bureau de machine virtuelle à utilisateur unique, par défaut, chaque imprimante virtuelle apparaît sous la forme *<printer_name>*(*vdi*). Dans un poste de travail publié ou une application publiée, par défaut, chaque imprimante virtuelle apparaît sous la forme *<printer_name>*(v*<session_ID>*).

À partir de Horizon Agent 7.12, vous pouvez utiliser une stratégie de groupe pour modifier la convention d'affectation de noms d'imprimante pour les imprimantes clientes qui sont redirigées. Pour plus d'informations, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon* pour votre version d'Horizon Agent.

Conditions préalables

Pour utiliser VMware Integrated Printing, un administrateur Horizon doit installer cette fonctionnalité sur le poste de travail distant. Cette tâche implique l'activation de l'option **VMware Integrated Printing** dans le programme d'installation d'Horizon Agent. Pour plus d'informations sur l'installation d'Horizon Agent, consultez le document *Configuration des postes de travail virtuels dans Horizon* ou *Configuration d'applications et de postes de travail publiés dans Horizon*. Pour plus d'informations sur la configuration de la fonctionnalité VMware Integrated Printing, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Pour déterminer si la fonctionnalité de VMware Integrated Printing est installée dans un poste de travail distant, vérifiez que les fichiers `C:\Program Files\Common Files\VMware\Remote Experience\x64\vmware-print-redir-server.exe` et `C:\Program Files\Common Files\VMware\Remote Experience\x64\vmware-print-redir-service.exe` existent dans le système de fichiers de poste de travail distant.

Cette fonctionnalité requiert Horizon Agent 7.7 ou version ultérieure.

Procédure

1. Dans le poste de travail distant Windows, accédez à **Panneau de configuration > Matériel et audio > Périphériques et imprimantes**.
2. Dans la fenêtre **Périphériques et imprimantes**, cliquez avec le bouton droit sur l'imprimante virtuelle et sélectionnez **Propriétés de l'imprimante** dans le menu contextuel.
3. Dans l'onglet **Général**, cliquez sur **Préférences**.
4. Dans la boîte de dialogue Options d'impression, sélectionnez les différents onglets et précisez les paramètres à utiliser.
5. Cliquez sur **OK** pour enregistrer les modifications.

Impression à partir d'un poste de travail distant vers une imprimante USB locale

Une imprimante USB est une imprimante qui est connectée à un port USB du système client local. Vous pouvez envoyer des travaux d'impression vers une imprimante USB connectée au système client local à partir d'un poste de travail distant.

Vous pouvez utiliser la fonctionnalité de redirection USB ou la fonctionnalité VMware Integrated Printing pour imprimer sur une imprimante USB à partir d'un poste de travail distant. Les imprimantes USB redirigées et les imprimantes virtuelles peuvent fonctionner ensemble sans conflit.

Utilisation de la fonctionnalité de redirection USB

Pour utiliser la fonctionnalité de redirection USB pour connecter une imprimante USB à un port USB virtuel dans un poste de travail distant, les pilotes d'imprimante requis doivent être installés sur le poste de travail distant, ainsi que sur le système client.

Lorsque vous utilisez la fonctionnalité de redirection USB pour rediriger une imprimante USB, l'imprimante USB n'est plus logiquement connectée au port USB physique du système client local et elle n'apparaît pas dans la liste des imprimantes locales du système client local. Vous pouvez imprimer sur une imprimante USB à partir du poste de travail distant, mais vous ne pouvez plus le faire sur une imprimante USB à partir du système client local.

Dans un poste de travail distant, les imprimantes USB redirigées apparaissent sous la forme *<printer_name>*.

Pour plus d'informations, reportez-vous à la section Utiliser des périphériques USB.

Utilisation de la fonctionnalité VMware Integrated Printing

Lorsque vous utilisez la fonctionnalité VMware Integrated Printing pour envoyer des travaux d'impression à une imprimante USB, vous pouvez imprimer sur l'imprimante USB à partir du poste de travail distant et du système client local. Vous n'avez pas besoin d'installer des pilotes d'imprimante dans le poste de travail distant.

Pour utiliser la fonctionnalité VMware Integrated Printing, celle-ci doit être activée lorsque vous installez Horizon Agent. Pour plus d'informations sur l'installation, reportez-vous au document *Configuration des postes de travail virtuels dans Horizon* ou *Configuration d'applications et de postes de travail publiés dans Horizon*.

Pour plus d'informations, reportez-vous à la section Définir les préférences d'impression de la fonctionnalité de VMware Integrated Printing.

Améliorer les performances de la souris sur un poste de travail distant

Si vous utilisez le protocole d'affichage VMware Blast ou PCoIP avec des applications 3D dans un poste de travail distant, les performances de la souris s'améliorent lorsque vous activez la fonctionnalité de souris relative.

Dans la plupart des cas, si vous utilisez des applications ne nécessitant pas le rendu 3D, Horizon Client transmet des informations sur les mouvements du pointeur de la souris à l'aide des coordonnées absolues. À l'aide des coordonnées absolues, le client convertit les mouvements de la souris localement, ce qui améliore les performances, en particulier si vous vous trouvez à l'extérieur du réseau d'entreprise.

Pour les tâches nécessitant l'utilisation d'applications gourmandes en ressources graphiques, telles qu'AutoCAD, ou pour jouer à des jeux vidéo 3D, vous pouvez améliorer les performances de la souris en activant la fonctionnalité de souris relative, qui utilise les coordonnées relatives plutôt que les coordonnées absolues.

Lorsque la fonction de souris relative est activée, les performances peuvent être lentes si vous vous trouvez à l'extérieur du réseau d'entreprise, sur un WAN.

Conditions préalables

Un administrateur Horizon doit activer le rendu 3D pour le pool de postes de travail. Pour plus d'informations sur les paramètres de pool et sur les options disponibles pour le rendu 3D, consultez le document *Configuration des postes de travail virtuels dans Horizon* ou *Configuration d'applications et de postes de travail publiés dans Horizon*.

Procédure

1. Démarrez Horizon Client et connectez-vous au serveur.
2. Cliquez avec le bouton droit sur le poste de travail distant et sélectionnez **VMware Blast** ou **PCoIP**.
3. Connectez-vous au poste de travail distant.
4. Sélectionnez **Options > Activer la souris relative** dans la barre de menus d'Horizon Client.

   L'option est une bascule. Pour désactiver la fonctionnalité de souris relative, sélectionnez à nouveau **Options > Activer la souris relative**.

   Note Si vous utilisez Horizon Client en mode fenêtré, plutôt qu'en mode Plein écran, et que la fonctionnalité de souris relative est activée, il est possible que vous ne puissiez pas déplacer le pointeur de la souris dans les options de menu Horizon Client ou déplacer le pointeur en dehors de la fenêtre Horizon Client. Pour résoudre cette situation, appuyez sur Ctrl+Alt.

Utilisation de scanners

Avec la fonctionnalité de redirection de scanner, vous pouvez scanner des informations dans les applications publiées et les postes de travail distants avec des scanners connectés au système client local. Cette fonctionnalité redirige les données d'analyse en utilisant une quantité de bande passante beaucoup plus faible que celle utilisée par la redirection USB.

La redirection de scanner prend en charge les périphériques d'analyse standard qui sont compatibles avec les formats TWAIN et WIA (Windows Image Acquisition). Les pilotes du scanner doivent être installés sur le système client local. Il n'est pas nécessaire d'installer les pilotes du scanner sur un poste de travail distant.

Si un administrateur Horizon a configuré la fonctionnalité de redirection de scanner et si vous utilisez le protocole d'affichage VMware Blast ou PCoIP, un scanner connecté à votre système client local peut être utilisé dans une application publiée ou un poste de travail distant.

Important Ne vous connectez pas à un scanner du menu **Connecter le périphérique USB** dans Horizon Client. Les performances seront inutilisables.

Lorsque les données d'analyse sont redirigées vers une application publiée ou un poste de travail distant, vous ne pouvez pas accéder au scanner sur l'ordinateur client local. Inversement, lorsqu'un scanner est utilisé sur l'ordinateur client local, vous ne pouvez pas y accéder via l'application publiée ou le poste de travail distant.

Un administrateur Horizon peut configurer les paramètres de stratégie de groupe pour contrôler les options disponibles dans la boîte de dialogue Préférences de redirection de VMware Horizon Scanner. Pour plus d'informations, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Note Si un administrateur Horizon configure la redirection de scanner pour qu'elle utilise un scanner spécifique et que le scanner n'est pas disponible, la redirection de scanner ne fonctionne pas.

Conseils pour l'utilisation de la fonctionnalité de redirection de scanner

- Pour modifier les paramètres de redirection de scanner, cliquez sur l'icône de scanner () dans la barre d'état système ou la zone de notification du poste de travail distant. Dans une application publiée, l'icône de la barre d'état système est redirigée vers l'ordinateur client local.

  Note Il n'est pas nécessaire d'utiliser le menu qui apparaît lorsque vous cliquez sur l'icône de scanner. La fonctionnalité de redirection de scanner fonctionne sans autre configuration. Si le menu ne répertorie aucun scanner, un scanner incompatible est connecté au système client local. Si l'icône de scanner n'apparaît pas, la fonctionnalité de redirection de scanner est désactivée ou n'est pas installée sur le poste de travail distant. L'icône de scanner ne s'affiche pas non plus sur les systèmes clients locaux qui ne prennent pas en charge cette fonctionnalité.

- Si vous voulez que la boîte de dialogue Propriétés de numérisation TWAIN s'affiche même si une application de numérisation ne présente pas la boîte de dialogue de numérisation, cliquez sur l'option **Préférences** dans le menu de l'icône du scanner et cochez la case **Forcer la boîte de dialogue des propriétés de numérisation TWAIN**.
- Pour afficher les noms de scanner réels plutôt que le scanner *nnn* VMware Virtual, cliquez sur l'option **Préférences** dans le menu de l'icône de scanner et cochez la case **Utiliser les noms définis par le fournisseur pour les scanners TWAIN**.

- Pour sélectionner des options de contrôle de compression d'image ou pour déterminer comment sélectionner le scanner par défaut, cliquez sur l'option **Préférences** dans le menu de l'icône de scanner, puis sélectionnez l'onglet **Compression** ou **Valeurs par défaut**.
- Si vous prévoyez d'utiliser la fonctionnalité Audio/Vidéo en temps réel pour rediriger les webcams conformément aux recommandations de VMware, cliquez sur l'option **Préférences** dans le menu de l'icône de scanner et cochez la case **Masquer les périphériques d'acquisition d'images de type webcam**.
- La plupart des scanners TWAIN affichent une boîte de dialogue des paramètres du scanner par défaut, mais pas tous. Pour les scanners qui n'affichent pas les options de paramètres, vous pouvez utiliser l'option **Préférences** dans le menu de l'icône du scanner et sélectionner l'option **Forcer la boîte de dialogue des propriétés de numérisation TWAIN**.
- Pour afficher la boîte de dialogue Propriétés du scanner TWAIN sur le poste de travail distant, cliquez sur l'option **Préférences** dans le menu de l'icône du scanner et cochez la case **Agent (boîte de dialogue Propriétés de numérisation de VMware)**. Pour afficher la boîte de dialogue Propriétés du scanner TWAIN sur le système client local, cochez la case **Client (boîte de dialogue Propriétés de numérisation native, si prise en charge)**.

  Note Dans la boîte de dialogue Propriétés du scanner TWAIN côté agent, certaines options moins courantes peuvent ne pas être incluses. Pour utiliser ces options moins courantes, cochez la case **Client (boîte de dialogue Propriétés de numérisation native, si prise en charge)**.

- La numérisation d'une image trop grande ou à une résolution trop élevée peut ne pas fonctionner. Dans ce cas, il se peut que l'indicateur de progression de la numérisation soit figé, ou que l'application de scanner se ferme de façon inattendue. Si vous réduisez le poste de travail distant, un message d'erreur peut s'afficher sur le système client local, vous avertissant que la résolution est trop élevée. Pour résoudre ce problème, réduisez la résolution ou recadrez l'image à une taille inférieure et numérisez-la à nouveau.

Redirection des ports série

Avec la fonctionnalité de redirection de port série, vous pouvez rediriger des ports série (COM) connectés localement, tels que les ports RS232 intégrés et les adaptateurs USB-série. Les périphériques comme les imprimantes, les lecteurs de code-barres et les autres périphériques série peuvent être connectés à ces ports et utilisés sur les postes de travail distants.

Si un administrateur Horizon a configuré la fonctionnalité de redirection de port série, et si vous utilisez le protocole d'affichage VMware Blast ou PCoIP, la redirection de port série fonctionne sur le poste de travail distant sans configuration supplémentaire. Par exemple, COM1 sur le système client local est redirigé en tant que COM1 sur le poste de travail distant. COM2 est redirigé en tant que COM2. Si le port COM est déjà en cours d'utilisation, il est mappé pour éviter les conflits. Par exemple, si COM1 et COM2 existent sur le poste de travail distant, COM1 sur le client est mappé vers COM3 par défaut.

Les pilotes de périphérique requis doivent être installés sur le système client local, mais vous n'avez pas besoin d'installer les pilotes de périphérique sur le poste de travail distant. Par exemple, si vous utilisez un adaptateur USB-série qui requiert des pilotes de périphérique spécifiques pour fonctionner sur votre système client local, vous devez installer ces pilotes uniquement sur le système client.

Important Si vous utilisez un périphérique qui se branche sur un adaptateur USB-série, ne connectez pas le périphérique depuis le menu **Connecter le périphérique USB** dans Horizon Client. En effet, cette opération achemine le périphérique via la redirection USB, et ignore la fonctionnalité de redirection de port série.

Conseils pour l'utilisation de la fonctionnalité de redirection de port série

- Cliquez sur l'icône de port série ( ) dans la barre d'état système ou la zone de notification du poste de travail distant pour connecter, déconnecter ou personnaliser les ports COM mappés.

  Lorsque vous cliquez sur l'icône de port série, le menu contextuel **Redirection série COM pour VMware Horizon** s'affiche. Si un administrateur a verrouillé la configuration, les éléments dans le menu contextuel sont estompés. L'icône s'affiche uniquement si un administrateur Horizon a configuré la fonctionnalité de redirection de port série et que toutes les exigences sont satisfaites. Pour plus d'informations, reportez-vous à la section Configuration système requise pour la redirection de port série.

- Dans le menu contextuel, les éléments de port sont répertoriés en tant que ***port* mappé au *port***, par exemple, **COM1 mappé sur COM3**. Le premier port, qui est COM1 dans cet exemple, est le port physique ou l'adaptateur USB-série sur le système client local. Le deuxième port, qui est COM3 dans cet exemple, est le port utilisé sur le poste de travail distant.

- Pour sélectionner la commande **Propriétés du port**, cliquez avec le bouton droit sur un port COM.

  Dans la boîte de dialogue Propriétés COM, vous pouvez configurer un port afin qu'il se connecte automatiquement lorsqu'une session de poste de travail distant est démarrée, ou ignorer DSR (le signal data-set-ready), ce qui est requis pour certains modems et d'autres périphériques.

  Vous pouvez également modifier le numéro de port que le poste de travail distant utilise. Par exemple, si le port COM1 sur le système client est mappé sur COM3 sur le poste de travail distant, mais que l'application que vous utilisez requiert COM1, vous pouvez modifier le numéro de port sur COM1. Si COM1 existe sur le poste de travail distant, vous pouvez voir **COM1 (chevauché)**. Vous pouvez toujours utiliser ce port chevauché. Le poste de travail distant peut recevoir des données série via le port depuis le serveur et depuis le système client.

- Connectez-vous à un port COM mappé avant d'essayer de lancer une application qui requiert un accès à ce port. Par exemple, cliquez avec le bouton droit sur un port COM et sélectionnez **Connecter** pour utiliser le port sur le poste de travail distant. Lorsque vous démarrez l'application, elle ouvre le port série.

  Lorsqu'un port COM redirigé est ouvert et utilisé sur un poste de travail distant, vous ne pouvez pas accéder au port sur l'ordinateur local. Inversement, lorsqu'un port COM est utilisé sur l'ordinateur local, vous ne pouvez pas y accéder sur le poste de travail distant.
- Sur le poste de travail distant, vous pouvez utiliser l'onglet **Paramètres du port** du Gestionnaire de périphériques Windows pour définir le débit en bauds par défaut d'un port COM particulier. Utilisez les mêmes paramètres dans le gestionnaire de périphériques Windows sur le système client. Les paramètres de cet onglet sont utilisés uniquement si l'application ne spécifie pas les paramètres du port.
- Avant de pouvoir déconnecter le port COM, vous devez le fermer dans l'application ou fermer l'application. Vous pouvez ensuite sélectionner la commande **Déconnecter** pour vous déconnecter et rendre le port COM physique disponible pour utilisation sur l'ordinateur client.
- Si vous configurez un port série pour qu'il se connecte automatiquement, que vous démarrez une application qui ouvre le port série, puis déconnectez et reconnectez la session de poste de travail, la fonctionnalité de connexion automatique n'est pas opérationnelle. Vous ne pouvez pas non plus vous connecter à l'aide de l'option de menu de l'icône de la barre d'état système du port série. Dans la plupart des cas, l'application ne peut plus utiliser le port série. Vous devez arrêter l'application, déconnecter la session de poste de travail et la reconnecter pour résoudre le problème.

Raccourcis clavier

Vous pouvez utiliser des raccourcis clavier pour des commandes de menu et des actions courantes.

Raccourcis clavier courants

Ces raccourcis clavier fonctionnent de la même manière dans Horizon Client que dans toutes les applications.

Tableau 5-1. Raccourcis clavier courants

Action	Touche ou combinaison de touches
Cliquer sur le bouton mis en surbrillance dans une boîte de dialogue	Appuyez sur Entrée.
Ouvrir le menu contextuel	Appuyez sur Maj+F10.
Cliquer sur le bouton **Annuler** dans une boîte de dialogue	Appuyez sur Échap.

Tableau 5-1. Raccourcis clavier courants (suite)

Action	Touche ou combinaison de touches
Naviguer entre les éléments de la fenêtre de la sélection de serveurs ou de la fenêtre de sélection des postes de travail et applications	Utilisez une touche fléchée pour vous déplacer dans la direction de la flèche. Pour déplacer vers la droite, appuyez sur la touche de tabulation. Pour déplacer vers la gauche, appuyez sur Maj + Tab.
Supprimer un élément de la fenêtre de sélection de serveurs ou de la fenêtre de sélection des postes de travail et applications	Appuyez sur Supprimer.
Dans Windows 8.x, naviguez entre la fenêtre **Démarrer** et la fenêtre du bureau distant	Appuyez sur la touche Windows.

Combinaisons de touches de la fenêtre de sélection de serveurs

Vous pouvez utiliser ces combinaisons de touches dans la fenêtre de sélection de serveurs dans Horizon Client.

Tableau 5-2. Combinaisons de touches de sélection de serveurs

Commande de menu ou action	Combinaison de touches
Ouvrir l'aide en ligne dans une fenêtre de navigateur	Alt+O+A, Ctrl+A
Commande **Nouveau serveur**	Alt+N
Ouvrir la fenêtre **Informations de support**	Alt+O+P
Ouvrir la fenêtre **À propos d'Horizon Client**	Alt+O+V
Commande **Configurer SSL**	Alt+O+O
Commande **Masquer le sélecteur après le lancement d'un élément**	Alt+O+M

Raccourcis clavier du sélecteur d'applications et postes de travail

Vous pouvez utiliser ces raccourcis clavier lorsque vous sélectionnez des applications publiées et des postes de travail distants dans Horizon Client.

Tableau 5-3. Raccourcis clavier du sélecteur d'applications et postes de travail

Commande de menu ou action	Combinaison de touches
Ouvrir l'aide en ligne dans une fenêtre de navigateur	Alt+O+A, Ctrl+A
Ouvrir le menu **Options**	Alt+O
Ouvrir la fenêtre **Informations de support**	Alt+O+P
Ouvrir la fenêtre **À propos d'Horizon Client**	Alt+O+V
Se déconnecter du poste de travail distant	Maj+F10+S

Tableau 5-3. Raccourcis clavier du sélecteur d'applications et postes de travail (suite)

Commande de menu ou action	Combinaison de touches
Se déconnecter et fermer la session du serveur	Alt+D
Basculer entre **Afficher les favoris** et **Tout afficher**	Alt+F
Pendant l'affichage des favoris, après la saisie des premiers caractères du nom de l'application publiée ou du poste de travail distant, accéder à l'élément suivant correspondant à la recherche	F4
Pendant l'affichage des favoris, accéder à l'élément précédent correspondant à la recherche	Maj+F4
Marquer comme favori ou supprimer une désignation de favori	Maj+F10+F
Ouvrir le menu **Paramètres**	Alt+S, ou Maj+F10+P
Démarrer l'élément sélectionné	Entrée ou Maj+F10+L
Épingler un raccourci pour le poste de travail distant ou une application publiée sur le menu Démarrer (pour Windows 7 et versions antérieures) ou la fenêtre Démarrer (pour Windows 8.x et versions ultérieures) sur le système client	Maj+F10+J
Ouvrir le menu contextuel **Paramètres d'affichage** du poste de travail distant sélectionné	Maj+F10+A
Utiliser le protocole d'affichage PCoIP pour se connecter au poste de travail distant sélectionné	Maj+F10+O
Utiliser le protocole d'affichage RDP pour se connecter au poste de travail distant sélectionné	Maj+F10+M
Créer un raccourci de poste de travail distant pour l'élément sélectionné	Maj+F10+C
Ajouter l'élément sélectionné au menu Démarrer ou à la fenêtre Démarrer	Maj+F10+J
Réinitialiser le poste de travail distant sélectionné (si votre administrateur vous permet de le réinitialiser)	Maj+F10+R
Actualiser la liste des postes de travail distants et des applications publiées	F5

Raccourcis de la fenêtre de poste de travail

Pour utiliser ces raccourcis, vous devez appuyer sur Ctrl+Alt ou cliquer sur la barre de menus d'Horizon Client, plutôt que cliquer à l'intérieur du poste de travail distant, avant d'appuyer sur les touches. Ces raccourcis fonctionnent uniquement lorsque vous utilisez le protocole d'affichage VMware Blast ou PCoIP.

Tableau 5-4. Raccourcis de la fenêtre de poste de travail distant

Commande de menu ou action	Combinaison de touches
Relâcher le curseur de la souris afin qu'il ne soit plus à l'intérieur du poste de travail distant	Ctrl+Alt
Ouvrir le menu **Options**	Alt+O
Ouvrir la fenêtre **Informations de support**	Alt+O+I
Ouvrir la fenêtre **À propos d'Horizon Client**	Alt+O+V
Ouvrir la boîte de dialogue Paramètres du dossier partagé	Alt+O+F
Basculer **Activer la mise à l'échelle de l'affichage**	Alt+O+N
Commande **Passer à un autre ordinateur de bureau**	Alt+O+P
Commande **Se connecter automatiquement à ce poste de travail**	Alt+O+N
Commande **Activer la souris relative**	Alt+O+T
Commande **Envoyer Ctrl+Alt+Suppr**	Alt+O+C
Commande **Déconnecter**	Alt+O+D
Commande **Déconnecter et fermer la session**	Alt+O+F
Commande **Connecter un périphérique USB**	Alt+U

Raccourcis clavier pour le focus d'entrée

Vous pouvez utiliser les paramètres de stratégie de groupe **Combinaison de touches de raccourci pour prendre le focus d'entrée** et **Combinaison de raccourcis pour libérer le focus d'entrée** pour configurer des raccourcis clavier pour le focus d'entrée. Vous pouvez utiliser le paramètre de stratégie de groupe **Focus d'entrée automatique dans une fenêtre de poste de travail virtuel** pour envoyer automatiquement l'entrée au poste de travail distant lorsqu'un utilisateur place le poste de travail distant au premier plan. Ces fonctionnalités sont utiles pour les utilisateurs qui ne peuvent pas utiliser les clics de souris pour saisir et libérer un poste de travail distant. Pour plus d'informations, reportez-vous à la section Paramètres généraux des objets de stratégie de groupe (GPO) de clients

Synchronisation de la langue source d'entrée du clavier

Lorsque vous vous connectez à un poste de travail distant, la langue source d'entrée du clavier sur le système client est synchronisée sur le poste de travail distant.

Cette fonctionnalité prend en charge les langues sources d'entrée du clavier suivantes sur le système client.

- Anglais

- Français
- Allemand
- Japonais
- Coréen
- Espagnol
- Chinois simplifié
- Chinois traditionnel

La synchronisation ne se produit pas si la langue source d'entrée du clavier n'est pas prise en charge.

La synchronisation de la langue source d'entrée du clavier est contrôlée par le paramètre de stratégie de groupe **Synchronisation des paramètres régionaux du clavier** côté agent. Pour plus d'informations, reportez-vous à la section « Paramètres de stratégie de groupe VMware Blast » dans le document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Configurer la synchronisation des touches de verrouillage

Vous pouvez configurer Horizon Client afin qu'il synchronise les états d'activation/de désactivation des touches Verrouillage numérique, Arrêt défilement et Verrouillage majuscule du système client vers un poste de travail distant en activant un paramètre dans Horizon Client. Ce paramètre est désactivé par défaut.

Vous pouvez également utiliser le paramètre de stratégie de groupe Horizon Client**Synchroniser automatiquement le pavé numérique, les touches Défil. et Verr. Maj.** pour configurer la synchronisation des touches de verrouillage. Lorsque ce paramètre de stratégie de groupe est activé ou désactivé, les utilisateurs ne peuvent pas modifier le paramètre de synchronisation des touches de verrouillage dans l'interface utilisateur de Horizon Client. Pour plus d'informations, reportez-vous à la section Paramètres généraux des objets de stratégie de groupe (GPO) de clients.

Si le paramètre de stratégie de groupe **Synchroniser automatiquement le pavé numérique, les touches Défil. et Verr. Maj.** est désactivé ou n'est pas configuré, ou le paramètre de synchronisation de la touche de verrouillage d'Horizon Client n'est pas sélectionné (paramètre par défaut), l'état du bouton bascule de la touche de verrouillage est synchronisé à partir du poste de travail distant sur le système client par défaut.

Procédure

1. Démarrez Horizon Client et connectez-vous à un serveur.
2. Ouvrez la boîte de dialogue Paramètres pour le poste de travail distant.
   - Cliquez sur l'icône **Paramètres** (engrenage) dans le coin supérieur droit de la fenêtre de sélection des postes de travail et applications, puis sélectionnez le poste de travail distant dans le volet de gauche.

- Cliquez avec le bouton droit sur le poste de travail distant de la fenêtre de sélection des postes de travail et applications et sélectionnez **Paramètres**.

3 Pour activer la fonctionnalité de synchronisation des touches de verrouillage, cochez la case **Synchroniser automatiquement le pavé numérique, les touches Défil. et Verr. Maj.**, puis cliquez sur **OK**.

Dépannage de Horizon Client 6

Vous pouvez résoudre la plupart des problèmes avec Horizon Client en redémarrant ou en réinitialisant les postes de travail distants ou les applications publiées, ou en réinstallant Horizon Client.

Ce chapitre contient les rubriques suivantes :

- Redémarrer un poste de travail distant
- Réinitialiser des postes de travail distants ou des applications publiées
- Réparer Horizon Client pour Windows
- Désinstaller Horizon Client pour Windows
- Problèmes avec la saisie au clavier
- Que faire si Horizon Client se ferme de façon inattendue
- Connexion à un serveur en mode Workspace ONE

Redémarrer un poste de travail distant

Si le système d'exploitation du poste de travail distant ne répond plus, vous devez redémarrer le poste de travail distant. Le redémarrage d'un poste de travail distant est similaire à la commande de redémarrage du système d'exploitation Windows. En général, le système d'exploitation du poste de travail distant demande d'enregistrer toutes les données non enregistrées avant de redémarrer.

Vous pouvez redémarrer un poste de travail distant uniquement si un administrateur Horizon a activé la fonctionnalité de redémarrage pour le poste de travail distant.

Pour plus d'informations sur l'activation de la fonctionnalité de redémarrage de poste de travail, consultez le document *Configuration des postes de travail virtuels dans Horizon* ou *Configuration d'applications et de postes de travail publiés dans Horizon*.

Procédure

- Utilisez la commande **Redémarrer le poste de travail**.

Option	Action
Depuis le poste de travail distant	Sélectionnez **Options > Redémarrer le poste de travail** dans la barre de menus.
Depuis la fenêtre de sélection des postes de travail	Cliquez avec le bouton droit de la souris sur l'icône du poste de travail distant, puis sélectionnez **Redémarrer le poste de travail**.

  Horizon Client vous invite à confirmer l'action de redémarrage.

Résultats

Le système d'exploitation du poste de travail distant redémarre et le client se déconnecte et ferme la session sur le poste de travail distant.

Étape suivante

Patientez jusqu'au redémarrage du système avant de tenter de vous reconnecter au poste de travail distant.

Si le redémarrage du poste de travail distant ne résout pas le problème, vous devrez peut-être réinitialiser le poste de travail distant. Reportez-vous à la section Réinitialiser des postes de travail distants ou des applications publiées.

Réinitialiser des postes de travail distants ou des applications publiées

Vous devez peut-être réinitialiser un poste de travail distant si le système d'exploitation du poste de travail cesse de répondre et que le redémarrage du poste de travail distant ne résout pas le problème.

La réinitialisation d'un poste de travail distant revient à appuyer sur le bouton Réinitialiser d'un ordinateur physique pour le forcer à redémarrer. Tous les fichiers ouverts sur le poste de travail distant sont fermés sans être enregistrés.

La réinitialisation d'applications publiées entraîne la fermeture de toutes les applications ouvertes.

Vous pouvez réinitialiser un poste de travail distant uniquement si un administrateur Horizon a activé la fonctionnalité de réinitialisation pour le poste de travail distant.

Pour plus d'informations sur l'activation de la fonctionnalité de réinitialisation de poste de travail, consultez le document *Configuration des postes de travail virtuels dans Horizon* ou *Configuration d'applications et de postes de travail publiés dans Horizon*.

Procédure

1 Pour réinitialiser un poste de travail distant, utilisez la commande **Réinitialiser le poste de travail**.

Option	Action
Depuis le poste de travail distant	Sélectionnez **Options > Réinitialiser le poste de travail** dans la barre de menu.
Depuis la fenêtre de sélection des postes de travail et applications	Cliquez avec le bouton droit sur l'icône du poste de travail distant, puis sélectionnez **Réinitialiser le poste de travail**.

2 Pour réinitialiser des applications publiées, utilisez le bouton **Réinitialiser** dans la fenêtre de sélection des postes de travail et applications.

   a Cliquez sur le bouton **Paramètres** (icône engrenage) dans la barre de menus.

   b Sélectionnez **Applications** dans le volet de gauche, cliquez sur le bouton **Réinitialiser** dans le volet de droite, puis cliquez sur **OK**.

Résultats

Lorsque vous réinitialisez un poste de travail distant, son système d'exploitation redémarre et le client se déconnecte et ferme la session. Lorsque vous réinitialisez des applications publiées, les applications publiées se ferment.

Étape suivante

Patientez jusqu'au redémarrage du système avant de tenter de vous reconnecter au poste de travail distant ou à l'application publiée.

Réparer Horizon Client pour Windows

Vous pouvez parfois résoudre des problèmes avec Horizon Client en réparant Horizon Client.

Conditions préalables

- Vérifiez que vous pouvez ouvrir une session en tant qu'administrateur sur le système client.
- Vérifiez que vous disposez du programme d'installation d'Horizon Client. Vous ne pouvez pas réparer Horizon Client si vous ne l'avez pas.

Procédure

- Pour réparer Horizon Client de manière interactive, effectuez l'une des tâches suivantes.
  - Double-cliquez sur le programme d'installation d'Horizon Client et cliquez sur **Réparer**.
  - Exécutez le programme d'installation d'Horizon Client à partir de la ligne de commande et entrez la commande `/repair`.

Par exemple, à l'invite de commande, tapez la commande suivante :

```
VMware-Horizon-Client-y.y.y-xxxxxx.exe /repair
```

y.y.y est le numéro de version et *xxxxxx* est le numéro de build.

- Pour réparer Horizon Client en mode silencieux, exécutez le programme d'installation d'Horizon Client à partir de la ligne de commande et entrez les commandes `/silent` et `/repair`.

  Par exemple, sur la ligne de commande, tapez la commande suivante :

  ```
  VMware-Horizon-Client-y.y.y-xxxxxx.exe /silent /repair
  ```

  y.y.y est le numéro de version et *xxxxxx* est le numéro de build.

Désinstaller Horizon Client pour Windows

Si la réparation d'Horizon Client ne résout pas le problème, vous devrez peut-être désinstaller et réinstaller Horizon Client.

Cette procédure montre comment désinstaller Horizon Client si vous disposez du programme d'installation d'Horizon Client.

Si vous ne disposez pas du programme d'installation d'Horizon Client, vous pouvez désinstaller Horizon Client de la même manière que vous désinstallez d'autres applications sur votre système Windows. Par exemple, sur un système Windows 10, vous pouvez utiliser la désinstallation de système d'exploitation Windows ou modifier une fonctionnalité de programme (**Panneau de configuration > Programmes et fonctionnalités > Désinstaller ou modifier un programme**).

Conditions préalables

Vérifiez que vous pouvez ouvrir une session en tant qu'administrateur sur le système client.

Procédure

- Pour désinstaller Horizon Client de manière interactive, effectuez l'une des tâches suivantes.
  - Double-cliquez sur le programme d'installation d'Horizon Client et cliquez sur **Supprimer**.
  - Exécutez le programme d'installation d'Horizon Client à partir de la ligne de commande et entrez la commande `/uninstall`.

    Par exemple, à l'invite de commande, tapez la commande suivante :

    ```
    VMware-Horizon-Client-y.y.y-xxxxxx.exe /uninstall
    ```

    y.y.y est le numéro de version et *xxxxxx* est le numéro de build.

- Pour désinstaller Horizon Client en mode silencieux, exécutez le programme d'installation d'Horizon Client à partir de la ligne de commande et entrez les commandes `/silent` et `/uninstall`.

  Par exemple, à l'invite de commande, tapez la commande suivante :

  ```
  VMware-Horizon-Client-y.y.y-xxxxxx.exe /silent /uninstall
  ```

  y.y.y est le numéro de version et *xxxxxx* est le numéro de build.

Étape suivante

Réinstallez Horizon Client. Reportez-vous à la section Chapitre 2 Installation d'Horizon Client pour Windows.

Problèmes avec la saisie au clavier

Lorsque vous saisissez du texte dans une application publiée ou un poste de travail distant, aucune des séquences de touches ne semble fonctionner.

Problème

Lorsque vous êtes connecté à une application publiée ou un poste de travail distant, aucun caractère ne s'affiche lorsque vous tapez. Vous pouvez également remarquer qu'une seule touche se répète sans cesse.

Cause

Certains logiciels de sécurité, tels que Norton 360 Total Security, incluent une fonction qui détecte les programmes enregistreurs de frappe et bloque la journalisation des séquences de touches. Cette fonction de sécurité permet de protéger le système contre les logiciels espions qui, par exemple, volent les mots de passe et les numéros de carte de crédit. Ce logiciel de sécurité peut empêcher Horizon Client d'envoyer des séquences de touches à l'application publiée ou au poste de travail distant.

Solution

- Sur le système client, désactivez la fonction de détection des enregistreurs de frappe de votre antivirus ou de votre logiciel de sécurité.

Que faire si Horizon Client se ferme de façon inattendue

Il arrive que Horizon Client se ferme sans que vous l'ayez demandé.

Problème

Horizon Client se ferme de façon inattendue. En fonction de la configuration du serveur, il est possible qu'un message tel que `Aucune connexion sécurisée au Serveur de connexion View` s'affiche. Parfois, aucun message n'apparaît.

Cause

Ce problème survient lorsque la connexion au serveur est perdue.

Solution

- Redémarrez Horizon Client. Vous pouvez parvenir à vous connecter lorsque le serveur est à nouveau en cours d'exécution. Si les problèmes de connexion persistent, contactez votre administrateur système ou le support de VMware.

Connexion à un serveur en mode Workspace ONE

Vous ne pouvez pas vous connecter à un serveur directement via Horizon Client ou votre poste de travail distant, et les droits d'accès à l'application publiée ne sont pas visibles dans Horizon Client.

Problème

- Lorsque vous tentez de vous connecter au serveur directement via Horizon Client, Horizon Client vous redirige vers le portail Workspace ONE.
- Lorsque vous ouvrez un poste de travail ou une application publiée via un URI ou un raccourci, ou lorsque vous ouvrez un fichier local via l'association de fichier, la demande vous redirige vers le portail Workspace ONE pour l'authentification.
- Lorsque vous ouvrez un poste de travail ou une application publiée via Workspace ONE et que Horizon Client démarre, vous ne pouvez pas voir ou ouvrir d'autres applications publiées ou postes de travail autorisés dans Horizon Client.

Cause

Un administrateur Horizon peut activer le mode Workspace ONE sur une instance du Serveur de connexion. Ce comportement est normal lorsque le mode Workspace ONE est activé sur une instance du Serveur de connexion.

Solution

Utilisez Workspace ONE pour vous connecter à un serveur compatible avec Workspace ONE et accéder à vos postes de travail distants et à vos applications publiées.