Utilisation de VMware Horizon Client pour Chrome OS

VMware Horizon Client for Chrome OS 4.5

FR-002506-00

vmware®

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

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

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

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

docfeedback@vmware.com

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

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

Table des matières

Utilisation de VMware Horizon Client pour Chrome OS

Ce guide, intitulé *Utilisation de VMware Horizon Client pour Chrome OS*, fournit des informations concernant l'installation et l'utilisation de VMware Horizon® Client™ pour Chrome OS sur un périphérique Chrome OS pour se connecter à une application ou à un poste de travail distant du centre de données.

Ce document contient des informations relatives aux configurations système requises ainsi que des instructions sur l'installation et l'utilisation d'Horizon Client pour Chrome OS.

Ces informations sont destinées aux administrateurs ayant déjà une certaine expérience de l'utilisation d'Horizon et de VMware vSphere. Si vous découvrez Horizon, vous devrez peut-être vous reporter aux instructions pas à pas pour réaliser les procédures de base dans les documents *Installation de View* et *Administration de View*.

1 Configuration et installation

La configuration d'un déploiement d'Horizon pour des clients Chrome OS implique l'utilisation de certains paramètres de configuration du Serveur de connexion, le respect de la configuration système requise pour les serveurs Horizon et les clients Chrome OS, ainsi que le téléchargement et l'installation d'Horizon Client pour Chrome OS.

À partir d'Horizon Client 4.3, vous pouvez installer Horizon Client pour Android sur certains modèles de Chromebook. Pour plus d'informations, consultez le document *Utilisation de VMware Horizon Client pour Android*.

Ce chapitre aborde les rubriques suivantes :

Configuration système requise

Le périphérique sur lequel vous installez Horizon Client doit se conformer à une certaine configuration système.

Modèles de périphérique	Chromebook
Systèmes d'exploitation	Chrome OS, version stable, ARC version 41.4410.244.13 ou ultérieure
Architecture du CPU	■ ARM ■ x86

Serveur de connexion, serveur de sécurité et View Agent ou Horizon Agent	Dernière version de maintenance de View 6.x et versions ultérieures. VMware recommande d'utiliser un serveur de sécurité ou un dispositif Unified Access Gateway pour que le périphérique ne nécessite pas de connexion VPN.
Protocoles d'affichage	■ PCoIP ■ VMware Blast (requiert Horizon Agent 7.0 ou version ultérieure)

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

L'Audio/Vidéo en temps réel fonctionne avec des périphériques audio standard et avec des applications de conférence standard, telles que Skype, WebEx et Google Hangouts. Pour prendre en charge la fonctionnalité Audio/Vidéo en temps réel, votre déploiement d'Horizon doit répondre à certaines exigences matérielles et logicielles.

Important Seule la fonctionnalité d'entrée audio est prise en charge. La fonctionnalité de vidéo n'est pas prise en charge.

Postes de travail distants	View Agent 5.3 ou version ultérieure doit être installé sur les postes de travail. S'agissant des postes de travail View Agent 5.3, la version correspondante de Remote Experience Agent doit également être installée sur les postes de travail. Par exemple, si View Agent 5.3 est installé, vous devez également installer Remote Experience Agent à partir de View 5.3 Feature Pack 1. Consultez le document *Installation et administration de View Feature Pack*. Si vous disposez de View Agent 6.0 ou version ultérieure, ou Horizon Agent 7.0 ou version ultérieure, aucun Feature Pack n'est requis. Pour utiliser l'Audio/Vidéo en temps réel avec des postes de travail RDS et des applications distantes, vous devez disposer d'Horizon Agent 7.0.2 ou version ultérieure.
Périphérique d'accès client	L'Audio/Vidéo en temps réel est pris en charge sur tous les Chromebooks qui exécutent Horizon Client pour Chrome OS.

Préparation du Serveur de connexion pour Horizon Client

Les administrateurs doivent effectuer des tâches spécifiques pour permettre aux utilisateurs finaux de se connecter à des applications ou des postes de travail distants.

Pour que les utilisateurs finaux puissent se connecter au Serveur de connexion ou à un serveur de sécurité et accéder à une application ou à un poste de travail distant, vous devez configurer un certain nombre de paramètres de pool et de sécurité :

- Si vous prévoyez d'utiliser Unified Access Gateway, configurez le Serveur de connexion pour qu'il fonctionne avec Unified Access Gateway. Reportez-vous au document *Déploiement et configuration d'Unified Access Gateway*. Les dispositifs Unified Access Gateway remplissent le même rôle que celui précédemment joué uniquement par des serveurs de sécurité.
- Si vous utilisez un serveur de sécurité, assurez-vous de disposer des dernières versions de maintenance du Serveur de connexion 5.3.x et du Serveur de sécurité 5.3.x ou versions ultérieures. Pour plus d'informations, reportez-vous au document *Installation de View*.
- Si vous prévoyez d'utiliser une connexion tunnel sécurisée pour des périphériques client et si la connexion sécurisée est configurée avec un nom d'hôte DNS pour le Serveur de connexion ou un serveur de sécurité, vérifiez que le périphérique client peut résoudre ce nom DNS.

Pour activer ou désactiver le tunnel sécurisé, dans Horizon Administrator, accédez à la boîte de dialogue Modifier les paramètres du Serveur de connexion Horizon et cochez la case **Utiliser une connexion par tunnel sécurisé vers le poste de travail**.

- 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, reportez-vous au document *Configuration des postes de travail virtuels dans Horizon 7* ou *Configuration d'applications et de postes de travail publiés dans Horizon 7*.
- Pour pouvoir utiliser une authentification à deux facteurs, telle que l'authentification RSA SecurID ou RADIUS, avec Horizon Client, vous devez activer cette fonctionnalité sur le Serveur de connexion. Pour plus d'informations, consultez les rubriques concernant l'authentification à deux facteurs dans le document *Administration de View*.
- Pour masquer les informations de sécurité dans Horizon Client, notamment les informations d'URL de serveur et le menu déroulant **Domaine**, activez les paramètres **Masquer les informations de serveur dans l'interface utilisateur client** et **Masquer la liste de domaines dans l'interface utilisateur client** dans Horizon Administrator. Ces paramètres globaux sont disponibles dans Horizon 7 versions 7.1 et ultérieures. Pour plus d'informations sur la configuration des paramètres globaux, consultez le document *Administration de View*.

  Pour s'authentifier lorsque le menu déroulant **Domaine** est masqué, les utilisateurs doivent fournir des informations sur le domaine en entrant leur nom d'utilisateur au format ***domaine**nomutilisateur*** ou ***utilisateur*nom@*domaine*** dans la zone de texte **Nom d'utilisateur**.

  Important Si vous activez les paramètres **Masquer les informations de serveur dans l'interface utilisateur client** et **Masquer la liste de domaines dans l'interface utilisateur client** et sélectionnez l'authentification à deux facteurs (RSA SecureID ou RADIUS) pour l'instance du Serveur de connexion, n'appliquez pas la correspondance des noms d'utilisateur Windows. L'application de la correspondance des noms d'utilisateur Windows empêchera les utilisateurs d'entrer des informations sur le domaine dans la zone de texte Nom d'utilisateur et la connexion échouera toujours. Pour plus d'informations, consultez les rubriques concernant l'authentification à deux facteurs dans le document *Administration de View*.
- Pour permettre aux utilisateurs d'accéder aux applications publiées dans Horizon Client sans avoir à s'authentifier, vous devez activer cette fonctionnalité dans le Serveur de connexion. Pour plus d'informations, consultez les rubriques concernant l'accès sans authentification dans le document *Administration de View*.

Utilisation de jetons logiciels RSA SecurID intégrés

Si vous créez et distribuez des jetons logiciels RSA SecurID aux utilisateurs finaux, ces derniers doivent entrer uniquement leur code d'identification personnel (PIN) et non pas le code PIN et un code de jeton pour s'authentifier.

Configuration requise

Vous pouvez utiliser le format CTF (Compressed Token Format) ou le provisionnement initial dynamique appelé CT-KIP (Cryptographic Token Key Initialization Protocol), pour configurer un système d'authentification RSA d'utilisation simple. Avec ce système, vous générez une URL à envoyer aux utilisateur finaux. Pour installer le jeton, les utilisateurs finaux collent directement cette URL dans Horizon Client sur leurs périphériques client. La boîte de dialogue permettant de coller l'URL s'affiche lorsque les utilisateurs finaux se connectent au Serveur de connexion avec Horizon Client.

Une fois le jeton logiciel installé, l'utilisateur final entre un code PIN pour s'authentifier. Avec des jetons RSA externes, les utilisateurs finaux doivent entrer un code PIN et le code de jeton généré par un jeton d'authentification matériel ou logiciel.

Les préfixes d'URL suivants sont pris en charge si les utilisateurs finaux font un copier-coller de l'URL dans Horizon Client lorsque Horizon Client est connecté à une instance du Serveur de connexion sur lequel RSA est activé :

- `viewclient-securid://`
- `http://127.0.0.1/securid/`

Les utilisateurs finaux peuvent installer le jeton en appuyant sur l'URL. Les préfixes `viewclient-securid://` et `http://127.0.0.1/securid/` sont pris en charge. Notez que tous les explorateurs ne prennent pas en charge les liens hypertextes qui commencent par `http://127.0.0.1`. En outre, certains explorateurs de fichiers, comme l'application File Manager sur la tablette ASUS Transformer Pad, ne peuvent pas lier le fichier SDTID à Horizon Client.

Pour plus d'informations sur l'utilisation du provisionnement initial dynamique ou le provisionnement (CTF) basé sur un fichier, voir la page Web *Jeton logiciel RSA SecurID pour les périphériques iPhone* sur http://www.rsa.com/node.aspx?id=3652 ou *Jeton logiciel RSA SecurID pour les périphériques Android* sur http://www.rsa.com/node.aspx?id=3832.

Instructions à l'attention des utilisateurs finaux

Lorsque vous créez une URL CTFString ou une URL CT-KIP pour l'envoyer aux utilisateurs finaux, vous pouvez générer une URL avec ou sans mot de passe ou code d'activation. Vous envoyez cette URL aux utilisateurs finaux dans un courrier électronique qui doit contenir les informations suivantes :

- Instructions d'accès à la boîte de dialogue d'installation d'un jeton logiciel.

  Instruction demandant aux utilisateurs finaux d'appuyer sur **Jeton externe** dans la boîte de dialogue Horizon Client qui les invite à entrer les informations d'identification de RSA SecurID lorsqu'ils se connectent à une instance du Serveur de connexion.

- L'URL CTFString ou l'URL CT-KIP en texte brut.

  Si l'URL est formatée, les utilisateurs finaux reçoivent un message d'erreur lorsqu'ils tentent de l'utiliser dans Horizon Client.

- Code d'activation si l'URL CT-KIP que vous créez ne contient pas le code d'activation.

  Les utilisateurs finaux doivent entrer ce code d'activation dans un champ de texte de la boîte de dialogue.

- Si l'URL CT-KIP contient un code d'activation, indiquez aux utilisateurs finaux qu'ils ne doivent rien entrer dans la zone de texte **Mot de passe ou code d'activation** dans la boîte de dialogue d'installation du jeton logiciel.

Configurer des options TLS/SSL avancées

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

TLSv1.0, TLSv1.1 et TLSv1.2 sont activés par défaut. SSL v2.0 et 3.0 ne sont pas pris en charge. La chaîne de contrôle de chiffrement par défaut est « !aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA +AESGCM:kECDH+AES:ECDH+AES:RSA+AES ».

Si vous configurez un protocole de sécurité pour Horizon Client qui n'est pas activé sur l'instance d'Horizon Server à laquelle le client se connecte, une erreur TLS/SSL se produit et la connexion échoue.

Pour obtenir des informations sur la configuration des protocoles de sécurité qui sont acceptés par les instances du Serveur de connexion, consultez le document *Sécurité de View*.

Procédure

1 Appuyez sur l'icône **Paramètres** (engrenage) dans le coin supérieur droit de la fenêtre Horizon Client, puis sur **Options de sécurité**.

2 Appuyez sur **Options SSL avancées**.

3 Assurez-vous que l'option **Utiliser les paramètres par défaut** n'est pas cochée.

4 Pour activer ou désactiver un protocole de sécurité, appuyez sur la case à cocher en regard du nom du protocole de sécurité.

5 Pour modifier la chaîne de contrôle de chiffrement, remplacez la chaîne par défaut.

6 (Facultatif) Si vous devez rétablir les paramètres par défaut, appuyez pour sélectionner l'option **Utiliser les paramètres par défaut**.

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

Vos modifications seront appliquées lors de votre prochaine connexion au serveur.

Systèmes d'exploitation de poste de travail pris en charge

Les administrateurs créent des machines virtuelles avec un système d'exploitation invité et installent le logiciel agent sur 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 de View*.

Installer ou mettre à niveau Horizon Client pour Chrome OS

Horizon Client pour Chrome OS est une application Chrome OS que vous installez comme n'importe quelle autre application Chrome OS.

Prérequis

Si vous n'avez pas encore configuré le périphérique Chrome OS, faites-le maintenant. Consultez le guide de l'utilisateur du fabricant de votre périphérique.

Procédure

1 Connectez-vous à votre Chromebook.

2 Téléchargez et installez l'application Horizon Client pour Chrome OS depuis le Chrome Web Store.

3 Pour savoir si l'installation a réussi, vérifiez que l'icône de l'application **Horizon Client pour Chrome OS** apparaît dans le Lanceur d'applications Chrome.

Configurer le décodage pour des sessions VMware Blast

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

Prérequis

Cette fonctionnalité requiert Horizon Agent 7.0 ou version ultérieure.

Procédure

1 Appuyez sur l'icône **Paramètres** (engrenage) dans le coin supérieur droit de l'écran Horizon Client et appuyez sur **VMware Blast**.

2 Cochez la case **H.264** pour autoriser le décodage H.264 ou décochez la case **H.264** pour le désactiver.

Lorsque la case est cochée, Horizon Client utilise le décodage H.264 si l'agent prend en charge le codage logiciel H.264. Si l'agent ne prend pas en charge le codage logiciel H.264, Horizon Client utilise le décodage JPG/PNG. Lorsque la case n'est pas cochée, Horizon Client utilise toujours le décodage JPG/PNG.

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

Configurer la vue par défaut d' Horizon Client

Vous pouvez configurer s'il convient ou non d'afficher les postes de travail et les applications récemment utilisés ou les raccourcis de serveur lorsque vous lancez Horizon Client.

Procédure

1 Appuyez sur l'icône **Paramètres** (engrenage) dans le coin supérieur droit de la fenêtre Horizon Client, puis sur **Affichage**.

2 Appuyez sur **Vue de lancement par défaut**.

La vue par défaut que vous avez sélectionnée prend effet immédiatement.

Activer la fonctionnalité de prise en charge de plusieurs moniteurs pour Horizon Client

Avec la fonctionnalité de prise en charge de plusieurs moniteurs, vous pouvez étendre un poste de travail distant à l'aide d'un moniteur externe.

Pour activer la prise en charge de plusieurs moniteurs pour Horizon Client, installez une extension d'assistance et activez le mode de poste de travail unifié sur votre Chromebook.

Lorsque l'écran du Chromebook et l'écran externe n'ont pas le même rapport largeur/longueur, vous devez installer l'extension d'assistance pour que la fenêtre du poste de travail distant s'affiche correctement sur le moniteur externe.

Procédure

1 Connectez-vous à votre Chromebook.

2 Téléchargez et installez l'extension d'assistance de VMware Horizon Client à partir de Chrome Web Store.

3 Ouvrez une fenêtre de navigateur dans votre Chromebook et tapez **`chrome://flags`** dans la barre d'URL.

4 Faites défiler jusqu'à **Mode de poste de travail unifié** et cliquez sur **Activer**.

5 Cliquez sur **Redémarrer maintenant** pour redémarrer votre Chromebook, afin que la modification prenne effet.

Suivant

Après le redémarrage du Chromebook, vous pouvez ouvrir les paramètres Chromebook et cliquer sur **Paramètres d'affichage** pour configurer les options d'affichage du poste de travail unifié.

Pour afficher une fenêtre du poste de travail distant sur le moniteur externe, cliquez sur le bouton **Agrandir**. Vous pouvez cliquer sur le bouton **Restaurer** pour que la fenêtre du poste de travail distant revienne sur le moniteur Chromebook.

Configuration d'une URL du Serveur de connexion par défaut

Un administrateur de Chrome peut configurer une URL du Serveur de connexion par défaut pour Horizon Client sur les Chromebooks inscrits. Lorsqu'une URL du Serveur de connexion est configurée par défaut, Horizon Client se connecte toujours au serveur par défaut.

Configuration requise et conditions préalables

La fonctionnalité d'URL du Serveur de connexion par défaut présente la configuration requise et les conditions préalables suivantes.

- La fonctionnalité est prise en charge uniquement sur les Chromebooks qui sont inscrits et gérés par la console d'administration G Suite.
- Un administrateur de Chrome doit installer l'application Horizon Client pour Chrome OS et l'extension d'assistance de VMware Horizon Client via la gestion du périphérique Chrome. L'application et l'extension sont disponibles dans le Chrome Web Store.

Lorsqu'une URL du Serveur de connexion est définie par défaut, les **paramètres** Horizon Client (icône d'engrenage) ne sont pas visibles avant qu'un utilisateur se connecte à une session à distance, et certains paramètres, tels que **VMware Blast** et **Accès non authentifié**, ne peuvent pas être modifiés.

Création d'un fichier de configuration JSON

Un administrateur de Chrome doit spécifier l'URL du Serveur de connexion par défaut dans un fichier de configuration JSON. Par exemple, le fichier de configuration JSON suivant définit l'URL du Serveur de connexion par défaut sur `connection-server.mycompany.com`.

```
{
    "Default Server URL":{
    "Value":"connection-server.mycompany.com"
   }
}
```

Les formats des URL suivants sont pris en charge.

Format	Exemple
Nom de domaine uniquement	`connexion-server.mycompanycom`
Nom de domaine et port	`connexion-server.mycompany.com:443`
Schéma HTTPS et nom de domaine	`https://connection-server.mycompany.com`
Schéma HTTPS, nom de domaine et nombre de ports	`https://connection-server.mycompany.com:443`

Création d'une stratégie pour définir l'URL du Serveur de connexion par défaut

Pour définir l'URL du Serveur de connexion pour les utilisateurs d'Horizon Client, un administrateur de Chrome doit créer une stratégie. Pour créer la stratégie, l'administrateur de Chrome doit se connecter à la console d'administration de Google, sélectionner l'extension d'assistance de VMware Horizon Client, sélectionner **Paramètres utilisateur**, puis télécharger le fichier de configuration JSON qui spécifie l'URL du Serveur de connexion par défaut.

Pour obtenir des informations détaillées sur l'utilisation de la console d'administration de Google, reportez-vous à l'aide de l'administrateur de G Suite.

Données Horizon Client collectées par VMware

Si votre entreprise participe au programme d'amélioration du produit, VMware collecte des données provenant de certains champs d'Horizon Client. Les champs contenant des informations sensibles restent anonymes.

VMware collecte des données sur les clients afin de hiérarchiser la compatibilité matérielle et logicielle. Si l'administrateur de votre entreprise a choisi de participer au programme d'amélioration du produit, VMware collecte des données anonymes sur votre déploiement afin d'améliorer la réponse de VMware aux exigences des clients. Aucune donnée permettant d'identifier votre organisation n'est collectée. Les informations d'Horizon Client sont envoyées d'abord au Serveur de connexion, puis à VMware, avec des données provenant des instances du Serveur de connexion, des pools de postes de travail et des postes de travail distants.

L'administrateur qui installe le Serveur de connexion peut choisir de participer au programme d'amélioration du produit VMware lors de l'exécution de l'assistant d'installation du Serveur de connexion, ou un administrateur peut définir une option dans Horizon Administrator 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 ?	Exemple
Entreprise ayant produit l'application Horizon Client	Non	VMware
Nom du produit	Non	VMware Horizon Client
Version du produit client	Non	(Le format est *x.x.x-yyyyyy*, où *x.x.x* est le numéro de version du client et *yyyyyy* est le numéro de build.)
Architecture binaire du client	Non	Exemples : ■ i386 ■ x86_64 ■ arm
Nom du build du client	Non	Exemples : ■ VMware-Horizon-Client-Win32-Windows ■ VMware-Horizon-Client-Linux ■ VMware-Horizon-Client-iOS ■ VMware-Horizon-Client-Mac ■ VMware-Horizon-Client-Android ■ VMware-Horizon-Client-WinStore
Système d'exploitation hôte	Non	Exemples : ■ Windows 8.1 ■ Windows 7, 64 bits Service Pack 1 (Build 7601) ■ iPhone OS 5.1.1 (9B206) ■ Ubuntu 12.04.4 LTS ■ Mac OS X 10.8.5 (12F45)
Noyau du système d'exploitation hôte	Non	Exemples : ■ Windows 6.1.7601 SP1 ■ Darwin Kernel Version 11.0.0: Sun Apr 8 21:52:26 PDT 2012; root:xnu-1878.11.10~1/RELEASE_ARM_S5L8945X ■ Darwin 11.4.2 ■ Linux 2.6.32-44-generic #98-Ubuntu SMP Mon Sep 24 17:27:10 UTC 2012 ■ inconnu (pour Windows Store)

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

Description	Ce champ reste-t-il anonyme ?	Exemple
Architecture du système d'exploitation hôte	Non	Exemples : ■ x86_64 ■ i386 ■ armv71 ■ ARM
Modèle du système hôte	Non	Exemples : ■ Dell Inc. OptiPlex 960 ■ iPad3,3 ■ MacBookPro8,2 ■ Dell Inc. Precision WorkStation T3400 (A04 03/21/2008)
Processeur du système hôte	Non	Exemples : ■ Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GH ■ Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GH ■ inconnu (pour iPad)
Nombre de cœurs dans le processeur du système hôte	Non	Par exemple : 4
Mo de mémoire sur le système hôte	Non	Exemples : ■ 4096 ■ inconnu (pour Windows Store)
Nombre de périphériques USB connectés	Non	2 (la redirection de périphériques USB est prise en charge uniquement pour les clients Linux, Windows et Mac.)
Nombre maximal de connexions de périphériques USB simultanées	Non	2
ID de fournisseur de périphériques USB	Non	Exemples : ■ Kingston ■ NEC ■ Nokia ■ Wacom
ID de produit de périphérique USB	Non	Exemples : ■ DataTraveler ■ Gamepad ■ Disque de stockage ■ Souris sans fil
Famille de périphériques USB	Non	Exemples : ■ Sécurité ■ Périphérique d'interface humaine ■ Imagerie
Nombre d'utilisations du périphérique USB	Non	(Nombre de partages du périphérique)

Gestion des connexions aux applications et postes de travail distants

2

Utilisez Horizon Client pour vous connecter à un serveur, pour modifier la liste des serveurs auxquels vous vous connectez, pour ouvrir ou fermer une session sur des postes de travail distants et pour utiliser des applications distantes. À des fins de dépannage, il vous permet également de réinitialiser les applications et postes de travail distants.

En fonction de la façon dont l'administrateur configure les stratégies de postes de travail distants, les utilisateurs finaux peuvent être en mesure d'exécuter plusieurs opérations sur leurs postes de travail.

Ce chapitre aborde les rubriques suivantes :

Définition du mode de vérification de certificats pour Horizon Client

Les administrateurs, et parfois les utilisateurs finaux, peuvent configurer le rejet des connexions client si une ou plusieurs vérifications de certificats de serveur échouent.

La vérification des certificats se produit pour les connexions SSL entre le Serveur de connexion et Horizon Client. La vérification de certificat inclut les vérifications suivantes :

- 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.

Remarque Pour plus d'informations sur la distribution d'un certificat racine auto-signé que les utilisateurs peuvent installer sur leurs périphériques Chrome OS, et sur l'installation d'un certificat sur un périphérique Chrome OS, consultez la documentation disponible sur le site Web de Google.

Pour définir le mode de sécurité, appuyez sur l'icône **Paramètres** (engrenage) dans le coin supérieur droit de la fenêtre Horizon Client, appuyez sur **Options de sécurité**, puis sur **Mode de sécurité**. Vous avez trois possibilités :

- **Ne jamais se connecter à des serveurs non autorisés**. Si l'une des vérifications de certificat échoue, le client ne peut pas se connecter au serveur. Un message d'erreur répertorie les vérifications qui ont échoué.
- **Signaler avant de se connecter à des serveurs non autorisés**. Si une vérification de certificat échoue car le serveur utilise un certificat auto-signé, vous pouvez cliquer sur **Continuer** pour ignorer l'avertissement. Pour les certificats auto-signés, le nom du certificat ne doit pas nécessairement correspondre au nom du serveur que vous avez entré dans Horizon Client.
- **Ne pas vérifier les certificats d'identité des serveurs**. Ce paramètre signifie qu'aucune vérification des certificats n'a lieu.

Si le mode de vérification des certificats est défini sur **Avertir**, vous pouvez toujours vous connecter à une instance du Serveur de connexion qui utilise un certificat auto-signé.

Si un administrateur installe ultérieurement un certificat de sécurité à partir d'une autorité de certification de confiance, afin que toutes les vérifications de certificat aient lieu 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.

Connexion à une application ou un poste de travail distant

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

Prérequis

- Procurez-vous des informations d'identification de connexion, telles que le nom d'utilisateur et le mot de passe Active Directory, le nom d'utilisateur et le code secret RSA SecurID ou le nom d'utilisateur et le code secret pour l'authentification RADIUS.
- Effectuez les tâches administratives décrites dans « Préparation du Serveur de connexion pour Horizon Client », page 8.
- Si vous vous trouvez à l'extérieur du réseau d'entreprise et si vous n'utilisez pas de serveur de sécurité pour accéder à l'application ou au poste de travail distant, vérifiez que votre périphérique client est configuré pour utiliser une connexion VPN et activez cette connexion.

  Important Dans la plupart des cas, utilisez un serveur de sécurité plutôt qu'un VPN.

- Vérifiez que vous disposez du nom de domaine complet (FQDN) du serveur qui fournit l'accès à l'application ou au poste de travail distant. 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 un logiciel RSA SecurID intégré, vérifiez que vous disposez de l'URL CT-KIP et du code d'activation corrects. Reportez-vous à la section « Utilisation de jetons logiciels RSA SecurID intégrés », page 9.
- Configurez le mode de vérification des certificats pour le certificat SSL présenté par le Serveur de connexion. Reportez-vous à la section « Définition du mode de vérification de certificats pour Horizon Client », page 17.

Procédure

1 Si une connexion VPN est requise, activez le VPN.

2 Sur votre périphérique Chrome OS, appuyez sur l'icône **Lanceur d'applications Chrome** dans la barre des tâches et appuyez sur l'application **Horizon Client pour Chrome OS**.

La fenêtre Horizon Client s'ouvre.

3 Connectez-vous à un serveur.

Option	Action
Se connecter à un nouveau serveur	Entrez le nom d'un serveur, entrez une description (facultative) et appuyez sur **Se connecter**.
Se connecter à un serveur existant	Appuyez sur le raccourci du serveur sur l'onglet **Serveurs**.

Les connexions entre Horizon Client et les serveurs utilisent toujours SSL. Le port par défaut pour les connexions SSL 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`**.

4 Si un message demande les informations d'identification RSA SecurID ou les informations d'identification pour l'authentification RADIUS, entrez les informations d'identification ou, si vous envisagez d'utiliser un jeton RSA SecurID intégré, installez un jeton intégré.

Option	Action
Jeton existant	Si vous utilisez un jeton d'authentification matériel ou logiciel sur un smartphone, entrez vos nom d'utilisateur et code secret. Le code secret peut comporter un code PIN et le numéro généré sur le jeton.
Installer le jeton logiciel	Cliquez sur **Jeton externe**. Dans la boîte de dialogue Installer le jeton logiciel, collez l'URL CT-KIP ou CTFString que votre administrateur vous a envoyée par e-mail. Si l'URL contient un code d'activation, vous n'avez rien à saisir dans la zone de texte **Mot de passe ou code d'activation**.

5 Si un message demande une seconde fois les informations d'identification RSA SecurID ou les informations d'identification pour l'authentification RADIUS, entrez le numéro généré suivant dans le jeton.

Ne saisissez pas votre code PIN ni le même numéro généré saisi précédemment. Si besoin, attendez qu'un autre numéro soit généré.

Cette étape n'est requise qu'en cas de mauvaise saisie du premier code secret ou lorsque les paramètres de configuration du serveur RSA changent.

6 Dans la boîte de dialogue d'ouverture de session, entrez votre nom d'utilisateur et votre mot de passe, sélectionnez un domaine et appuyez sur **Se connecter**.

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

7 (Facultatif) Appuyez sur l'icône des paramètres du protocole d'affichage dans le coin supérieur droit de l'écran pour sélectionner le protocole d'affichage à utiliser.

VMware Blast améliore l'autonomie de la batterie. Il s'agit du meilleur protocole pour les utilisateurs de périphériques 3D et mobiles haut de gamme. Le protocole d'affichage par défaut est **PCoIP**.

8 Appuyez sur l'icône d'une application ou d'un poste de travail distant pour vous y connecter.

Après votre première connexion à une application ou un poste de travail distant, un raccourci pour le poste de travail ou l'application en question est sauvegardé dans l'onglet **Récent**. La prochaine fois que vous voulez vous connecter à l'application ou au poste de travail distant, vous pouvez appuyer sur ce raccourci.

Si Horizon Client ne parvient pas à se connecter au poste de travail distant, effectuez les tâches suivantes :

- Déterminez si le Serveur de connexion est configuré pour ne pas utiliser SSL. Horizon Client requiert des connexions SSL. Vérifiez si le paramètre général dans Horizon Administrator de la case **Utiliser SSL pour les connexions client** est désélectionné. Si c'est le cas, vous devez cocher la case pour que SSL soit utilisé ou configurer votre environnement de sorte que les clients puissent se connecter à un équilibrage de charge activé pour HTTPS ou à un autre périphérique intermédiaire configuré pour établir une connexion HTTP vers le Serveur de connexion.
- Vérifiez que le certificat de sécurité pour le Serveur de connexion fonctionne correctement. Si ce n'est pas le cas, dans Horizon Administrator, l'agent sur des postes de travail ne sera peut-être pas accessible.
- Vérifiez que les balises définies sur l'instance du Serveur de connexion autorisent les connexions depuis cet utilisateur. Reportez-vous au document *Administration de View*.
- Vérifiez que l'utilisateur est autorisé à accéder à ce poste de travail ou à cette application. Reportez-vous au document *Configuration des postes de travail virtuels dans Horizon 7* ou *Configuration d'applications et de postes de travail publiés dans Horizon 7*.

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

Un administrateur Horizon peut utiliser la fonctionnalité Accès non authentifié pour créer des utilisateurs avec un accès non authentifié et autoriser ces utilisateurs à accéder à des applications distantes sur une instance du Serveur de connexion. Les utilisateurs avec un accès non authentifié peuvent se connecter au serveur de façon anonyme pour se connecter à leurs applications distantes.

Prérequis

- Effectuez les tâches administratives décrites dans « Préparation du Serveur de connexion pour Horizon Client », page 8.
- 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 de View*.
- Configurez le mode de vérification des certificats pour le certificat SSL présenté par le Serveur de connexion. Reportez-vous à la section « Définition du mode de vérification de certificats pour Horizon Client », page 17.
- Si vous accédez à des applications distantes à l'extérieur du réseau d'entreprise, vérifiez que votre périphérique client est configuré pour utiliser une connexion VPN et activez cette connexion.

Procédure

1 Si une connexion VPN est requise, activez le VPN.

2 Sur votre périphérique Chrome OS, appuyez sur l'icône Lanceur d'applications Chrome dans la barre des tâches et appuyez sur l'application Horizon Client pour Chrome OS.

La fenêtre Horizon Client s'ouvre.

3 Appuyez sur l'icône **Paramètres** (engrenage) dans le coin supérieur droit de la fenêtre Horizon Client, appuyez sur **Accès non authentifié** et cochez la case **Accès non authentifié**.

4 Connectez-vous au serveur sur lequel vous disposez d'un accès non authentifié à des applications distantes.

Option	Description
Se connecter à un nouveau serveur	Entrez le nom d'un serveur, entrez une description (facultative) et appuyez sur **Se connecter**.
Se connecter à un serveur existant	Appuyez sur le raccourci du serveur sur l'onglet **Serveurs**.

Les connexions entre Horizon Client et les serveurs utilisent toujours SSL. Le port par défaut pour les connexions SSL 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`.

5 Lorsque la fenêtre de connexion s'affiche, sélectionnez un compte d'utilisateur dans le menu déroulant **Compte d'utilisateur**, si nécessaire.

Si un seul un compte d'utilisateur est disponible, le compte d'utilisateur est automatiquement sélectionné.

6 (Facultatif) Cochez la case **Toujours utiliser ce compte** pour contourner la fenêtre de connexion lors de votre prochaine connexion au serveur.

Pour décocher ce paramètre avant votre prochaine connexion au serveur, appuyez longuement sur le raccourci du serveur jusqu'à ce que le menu contextuel s'affiche, appuyez sur **Modifier**, puis sur **Oublier le compte d'accès non authentifié enregistré (*nom*)** et enfin sur **Terminé**.

7 Appuyez sur **Connexion** pour vous connecter au serveur.

La fenêtre de sélection des applications s'affiche.

8 Appuyez sur l'icône de l'application pour démarrer l'application.

Après votre première connexion à une application distante, un raccourci pour l'application en question est enregistré dans l'onglet **Récent**. La prochaine fois que vous souhaiterez vous connecter à l'application distante, il vous suffira d'appuyer sur le raccourci au lieu d'appuyer sur l'icône du serveur.

Gérer les raccourcis de serveur

Une fois que vous êtes connecté à un serveur, Horizon Client crée un raccourci de serveur. Vous pouvez modifier et supprimer les raccourcis de serveurs.

Horizon Client enregistre le nom du serveur ou l'adresse IP dans un raccourci, même si vous avez tapé une adresse IP ou un nom de serveur incorrect. Vous pouvez supprimer ou modifier ces informations en modifiant le nom du serveur ou l'adresse IP. Si vous n'entrez pas de description de serveur, le nom ou l'adresse IP du serveur devient la description par défaut.

Procédure

1 Dans l'onglet **Serveurs**, appuyez longuement sur le raccourci du serveur jusqu'à ce que le menu contextuel s'affiche.

2 Utilisez le menu contextuel pour supprimer le serveur ou modifier le nom du serveur, la description du serveur ou le nom de l'utilisateur.

3 Si vous avez modifié le raccourci du serveur, appuyez sur **Terminé** pour enregistrer vos modifications.

Sélectionner une application ou un poste de travail distant favori

Vous pouvez sélectionner des postes de travail et des applications distants comme favoris. Les favoris sont identifiés par une étoile. L'étoile vous permet de trouver rapidement vos applications et postes de travail favoris. Vos sélections favorites sont sauvegardées, même après la fermeture de votre session sur le serveur.

Prérequis

Obtenez les informations d'identification dont vous avez besoin pour vous connecter au serveur, telles qu'un nom d'utilisateur et un mot de passe ou un jeton RSA SecurID et un code secret.

Procédure

1 Dans l'onglet **Serveurs**, appuyez sur le raccourci du serveur.

2 Si vous y êtes invité, entrez votre nom d'utilisateur et code secret RSA, votre nom d'utilisateur et mot de passe Active Directory, ou les deux.

3 Procédez comme suit pour sélectionner ou désélectionner un poste de travail ou une application comme favori.

Option	Description
Sélectionner un favori	Dans l'onglet **Tout**, appuyez longuement sur le nom du poste de travail ou de l'application jusqu'à ce que le menu contextuel s'affiche, puis appuyez sur **Marquer comme favori**. Une étoile s'affiche dans le coin supérieur droit du nom et le nom s'affiche dans l'onglet **Favoris**.
Désélectionner un favori	Dans l'onglet **Tout** ou **Favoris**, appuyez longuement sur le nom du poste de travail ou de l'application jusqu'à ce que le menu contextuel s'affiche, puis appuyez sur **Supprimer des favoris**. Une étoile ne s'affiche plus dans le coin supérieur droit du nom et le nom disparaît de l'onglet **Favoris**.

4 Pour afficher uniquement les applications et les postes de travail favoris, appuyez sur l'onglet **Favoris**.

Vous pouvez appuyer sur l'onglet **Tout** pour afficher tous les postes de travail et toutes les applications disponibles.

Déconnexion d'une application ou d'un poste de travail distant

Vous pouvez vous déconnecter d'un poste de travail distant sans fermer votre session afin que les applications restent ouvertes sur le poste de travail distant. Vous pouvez également vous déconnecter d'une application distante de manière que celle-ci reste ouverte.

Lorsque vous êtes connecté à l'application ou au poste de travail distant, vous pouvez vous déconnecter en appuyant sur l'icône **Se déconnecter** dans la barre latérale Unity Touch.

Remarque Un administrateur Horizon peut configurer votre poste de travail pour que la session soit fermée automatiquement lors de la déconnexion. Dans ce cas, tous les programmes ouverts sur votre poste de travail sont arrêtés.

Fermer une session sur un poste de travail distant

Vous pouvez fermer une session sur un système d'exploitation de poste de travail distant, même si aucun poste de travail n'est ouvert dans Horizon Client.

Si vous êtes actuellement connecté à un poste de travail distant et que vous y avez ouvert une session, vous pouvez utiliser le menu **Démarrer** de Windows pour fermer la session. Après que Windows a fermé votre session, le poste de travail est déconnecté.

Remarque Tous les fichiers non enregistrés qui sont ouverts sur le poste de travail distant sont fermés lors de l'opération de fermeture de session.

Prérequis

- Obtenez les informations d'identification dont vous avez besoin pour ouvrir une session, telles que le nom d'utilisateur et le mot de passe Active Directory, le nom d'utilisateur et le code secret RSA SecurID ou le nom d'utilisateur et le code secret pour l'authentification RADIUS.
- Si vous n'avez encore jamais ouvert de session, familiarisez-vous avec la procédure « Connexion à une application ou un poste de travail distant », page 18.

Procédure

1 Dans l'onglet **Serveurs**, appuyez sur le raccourci du serveur.

2 Si vous y êtes invité, entrez votre nom d'utilisateur et code secret RSA, votre nom d'utilisateur et mot de passe Active Directory, ou les deux.

3 Dans l'onglet **Tous**, appuyez longuement sur le raccourci du poste de travail jusqu'à ce que le menu contextuel s'affiche.

   Si le poste de travail est un favori, vous pouvez également exécuter cette étape dans l'onglet **Favoris**.

4 Appuyez sur **Fermer la session** dans le menu contextuel.

Suivant

Appuyez sur la flèche Précédent dans le coin supérieur gauche de la fenêtre Horizon Client, ou sur l'icône **Se déconnecter** dans le coin supérieur droit de la fenêtre Horizon Client, et appuyez sur **Fermer la session** pour vous déconnecter du serveur.

Gérer les raccourcis de poste de travail et d'application

Une fois que vous êtes connecté à une application ou à un poste de travail distant, Horizon Client enregistre un raccourci pour l'application ou le poste de travail récemment utilisé. Vous pouvez réorganiser et supprimer ces raccourcis.

Procédure

- Effectuez ces étapes pour supprimer un raccourci de poste de travail ou d'application de l'onglet **Récent**.

  a Appuyez longuement sur le raccourci jusqu'à ce que **Supprimer le raccourci** s'affiche en bas de la fenêtre.

  b Faites glisser le raccourci vers **Supprimer le raccourci**.

- Pour déplacer un raccourci de poste de travail ou d'application, faites-le glisser vers le nouvel emplacement.

Utilisation d'une application ou d'un poste de travail distant sur un périphérique Chrome OS

3

Sur les périphériques Chrome OS, Horizon Client inclut des fonctions supplémentaires pour faciliter la navigation.

Ce chapitre aborde les rubriques suivantes :

Matrice de prise en charge des fonctions

Certaines fonctionnalités ne sont pas disponibles lorsque vous accédez à un poste de travail distant à partir d'Horizon Client pour Chrome OS.

Tableau 3-1. Fonctionnalités prises en charge sur les postes de travail Windows pour Horizon Client pour Chrome OS

Fonction	Poste de travail Windows 10	Poste de travail Windows 8.x	Poste de travail Windows 7	Poste de travail Windows XP	Poste de travail Windows Vista	Poste de travail Windows Server 2008/2012 R2 ou Windows Server 2016
RSA SecurID ou RADIUS	X	X	X	Limité	Limité	X
Authentification unique	X	X	X	Limité	Limité	X
Protocole d'affichage RDP						
Protocole d'affichage PCoIP	X	X	X	Limité	Limité	X

Tableau 3-1. Fonctionnalités prises en charge sur les postes de travail Windows pour Horizon Client pour Chrome OS (suite)

Fonction	Poste de travail Windows 10	Poste de travail Windows 8.x	Poste de travail Windows 7	Poste de travail Windows XP	Poste de travail Windows Vista	Poste de travail Windows Server 2008/2012 R2 ou Windows Server 2016
Protocole d'affichage VMware Blast	X	X	X			X
redirection USB						
Redirection de lecteur client						
Audio/Vidéo en temps réel (entrée audio uniquement)	X	X	X			X
Wyse MMR						
Redirection multimédia (MMR) Windows 7						
Impression virtuelle						
Impression basée sur l'emplacement	X	X	X	Limité	Limité	X
Cartes à puce						
Plusieurs écrans	X	X	X	Limité	Limité	X

Les postes de travail Windows 10 requièrent View Agent 6.2 ou version ultérieure, ou Horizon Agent 7.0 ou version ultérieure. Les postes de travail Windows Server 2012 R2 requièrent View Agent 6.1 ou version ultérieure. Les postes de travail Windows Server 2016 requièrent Horizon Agent 7.0.2 ou version ultérieure.

Important View Agent 6.1 et versions ultérieures et Horizon Agent 7.0 et versions ultérieures ne prennent pas en charge les postes de travail Windows XP et Windows Vista. View Agent 6.0.2 est la dernière version de View qui prend en charge ces systèmes d'exploitation. Les clients qui disposent d'un contrat de support étendu avec Microsoft pour Windows XP et Vista, ainsi qu'un contrat de support étendu avec VMware pour ces systèmes d'exploitation invités, peuvent déployer l'instance de View Agent 6.0.2 de leurs postes de travail Windows XP et Vista avec le Serveur de connexion 6.1.

Pour une description de ces fonctionnalités et de leurs limites, consultez le document *Planification de l'architecture de View*.

Fonctionnalités prises en charge pour les postes de travail publiés sur les hôtes RDS

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

Remarque Le tableau suivant contient des lignes uniquement pour les fonctionnalités prises en charge. Lorsque le texte spécifie une version minimale de View Agent, le texte « et versions ultérieures » s'entend « inclure Horizon Agent 7.0.x et versions ultérieures ».

Tableau 3-2. Fonctionnalités prises en charge par les hôtes RDS avec View Agent 6.0.x ou version ultérieure, ou Horizon Agent 7.0.x ou version ultérieure, installé

Fonction	Hôte RDS Windows Server 2008 R2	Hôte RDS Windows Server 2012	Hôte RDS Windows Server 2016
RSA SecurID ou RADIUS	X	X	Horizon Agent 7.0.2 et versions ultérieures
Authentification unique	X	X	Horizon Agent 7.0.2 et versions ultérieures
Protocole d'affichage PCoIP	X	X	Horizon Agent 7.0.2 et versions ultérieures
Protocole d'affichage VMware Blast	Horizon Agent 7.0 et version ultérieure	Horizon Agent 7.0 et version ultérieure	Horizon Agent 7.0.2 et versions ultérieures
HTML Access	View Agent 6.0.2 et versions ultérieures (machine virtuelle uniquement)	View Agent 6.0.2 et versions ultérieures (machine virtuelle uniquement)	Horizon Agent 7.0.2 et versions ultérieures
Impression virtuelle (pour clients de poste de travail)	View Agent 6.0.1 et versions ultérieures (machine virtuelle uniquement)	View Agent 6.0.1 et versions ultérieures (machine virtuelle uniquement)	Horizon Agent 7.0.2 et versions ultérieures (machine virtuelle uniquement)
Impression basée sur l'emplacement	View Agent 6.0.1 et versions ultérieures (machine virtuelle uniquement)	View Agent 6.0.1 et versions ultérieures (machine virtuelle uniquement)	Horizon Agent 7.0.2 et versions ultérieures (machine virtuelle uniquement)
Plusieurs moniteurs (pour clients de poste de travail)	X	X	Horizon Agent 7.0.2 et versions ultérieures
Unity Touch (pour les clients Chrome OS et mobiles)	X	X	Horizon Agent 7.0.2 et versions ultérieures
Audio/Vidéo en temps réel (RTAV)	Horizon Agent 7.0.2 et versions ultérieures	Horizon Agent 7.0.2 et versions ultérieures	Horizon Agent 7.0.3 et versions ultérieures

Pour plus d'informations sur les éditions de chaque système d'exploitation invité et les service packs pris en charge, consultez le document *Installation de View*.

Pour plus d'informations sur les exigences de l'Audio/Vidéo en temps réel (RTAV), consultez la section « Configuration système requise pour l'Audio/Vidéo en temps réel », page 8.

Mouvements

VMware a créé des aides d'interaction utilisateur pour faciliter la navigation dans les éléments de l'interface utilisateur Windows classique sur un périphérique non-Windows.

Clic

Comme dans les autres applications, vous pouvez appuyer sur votre pavé tactile pour cliquer sur un élément de l'interface utilisateur. Si votre périphérique Chrome OS a un écran tactile, vous pouvez appuyer pour cliquer sur un élément de l'interface utilisateur. Vous pouvez également utiliser une souris externe.

Clic droit

Les options suivantes sont disponibles pour le clic droit :

- Appuyez avec deux doigts sur le pavé tactile.
- Maintenez la touche Alt enfoncée sur le clavier et appuyez sur le pavé tactile avec un doigt.

- Utilisez une souris externe pour faire un clic droit.
- Si votre périphérique Chrome OS dispose d'un écran tactile, appuyez avec deux doigts à peu près en même temps. Le clic droit se produit à l'endroit où le premier doigt a exercé une pression.

Défilement et barres de défilement

Les options suivantes sont disponibles pour le défilement vertical.

- Appuyez longuement avec votre pouce et faites défiler vers le bas avec un doigt sur le pavé tactile. Vous pouvez également faire défiler avec deux doigts.
- Utilisez une souris externe pour faire défiler.
- Si votre périphérique Chrome OS dispose d'un écran tactile, appuyez avec un ou deux doigts, puis faites glisser pour faire défiler. Le texte sous vos doigts se déplace dans la même direction que vos doigts. Le défilement avec un doigt ne fonctionne pas si vous avez effectué un zoom avant ou lorsque le clavier à l'écran est affiché.

Zoom avant et arrière

Comme dans les autres applications, utilisez votre clavier et appuyez sur Ctrl et + pour effectuer un zoom avant et sur Ctrl et - pour effectuer un zoom arrière. Si votre périphérique Chrome OS dispose d'un écran tactile, vous pouvez écarter vos doigts pour effectuer un zoom arrière et les rapprocher pour effectuer un zoom avant.

Redimensionnement de fenêtre

Pour utiliser le pavé tactile pour redimensionner une fenêtre, appuyez avec un doigt dans le coin ou sur le côté de la fenêtre et faites-le glisser pour redimensionner. Si votre périphérique Chrome OS dispose d'une souris externe, placez le curseur sur le bord de la fenêtre et faites-le glisser pour agrandir ou rétrécir la fenêtre. Vous ne pouvez pas redimensionner la fenêtre si elle est agrandie.

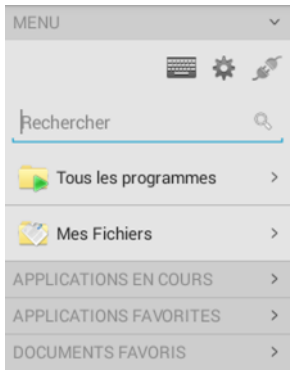
Son, musique et vidéo

Si le son est activé sur le périphérique, vous pouvez écouter des fichiers audio sur un poste de travail distant.

Utilisation de la barre latérale Unity Touch avec un poste de travail distant

Vous pouvez accéder rapidement à une application ou un fichier de poste de travail distant à partir de la barre latérale Unity Touch. À partir de cette barre latérale, vous pouvez ouvrir des fichiers et des applications, basculer entre des applications en cours d'exécution, et réduire, agrandir, restaurer ou fermer des fenêtres et des applications dans un poste de travail distant.

Figure 3-1. Barre latérale Unity Touch pour un poste de travail distant



À partir de cette barre latérale, vous pouvez réaliser plusieurs actions sur un fichier ou une application.

Tableau 3-3. Actions de la barre latérale Unity Touch pour un poste de travail distant

Action	Procédure
Afficher ou masquer le clavier à l'écran	Appuyez sur l'icône **Clavier**.
Modifier les paramètres d'Horizon Client	Appuyez sur l'icône **Paramètres**.
Se déconnecter du poste de travail	Appuyez sur l'icône **Se déconnecter**.
Afficher la barre latérale	Faites glisser la barre latérale vers la droite ou appuyez sur l'onglet de la barre latérale.
Masquer la barre latérale	Faites glisser la barre latérale vers la gauche ou appuyez sur la zone du poste de travail.
Accéder à une application	Appuyez sur **Tous les programmes** et accédez à l'application comme vous le feriez à partir du menu Démarrer de Windows.
Accéder à un fichier	Appuyez sur **Mes fichiers** pour accéder au dossier `Utilisateur` et accédez au fichier. **Mes fichiers** contient des dossiers tels que `Mes images`, `Mes documents` et `Téléchargements`. **Mes fichiers** contient les dossiers dans le profil d'utilisateur (répertoire `%USERPROFILE%`). Si vous déplacez le dossier `system` dans le répertoire `%USERPROFILE%`, le menu **Mes fichiers** peut également afficher le contenu du dossier déplacé, qu'il s'agisse d'un dossier déplacé local ou d'un dossier partagé sur un réseau.
Rechercher une application ou un fichier	■ Appuyez dans la zone **Rechercher** et saisissez le nom de l'application ou du fichier. ■ Pour utiliser la dictée vocale, appuyez sur le microphone sur le clavier. ■ Pour lancer une application ou un fichier, appuyez sur le nom de l'application ou du fichier dans les résultats de la recherche. ■ Pour revenir à l'accueil de la barre latérale, appuyez sur **X** pour fermer la zone **Rechercher**.
Ouvrir une application ou un fichier	Appuyez sur le nom du fichier ou de l'application dans la barre latérale. L'application démarre et la barre latérale se ferme.
Basculer entre des applications en cours d'exécution ou ouvrir des fenêtres	Appuyez sur le nom de l'application sous **Applications en cours d'exécution**. Si plusieurs fichiers sont ouverts pour une application, appuyez sur le chevron (>) à côté de l'application pour développer la liste.
Réduire une fenêtre ou une application en cours d'exécution	Appuyez longuement sur le nom de l'application sous **Applications en cours d'exécution** jusqu'à ce que le menu contextuel s'affiche. Appuyez sur **Réduire**.
Agrandir une fenêtre ou une application en cours d'exécution	Appuyez longuement sur le nom de l'application sous **Applications en cours d'exécution** jusqu'à ce que le menu contextuel s'affiche. Appuyez sur **Agrandir**.
Fermer une application en cours d'exécution ou une fenêtre	Appuyez longuement sur le nom de l'application sous **Applications en cours d'exécution** jusqu'à ce que le menu contextuel s'affiche. Appuyez sur **Fermer**.
Rétablir une fenêtre ou une application en cours d'exécution à sa taille et sa position précédentes	Appuyez longuement sur le nom de l'application sous **Applications en cours d'exécution** jusqu'à ce que le menu contextuel s'affiche. Appuyez sur **Restaurer**.
Créer une liste d'applications ou de fichiers favoris	1 Recherchez l'application ou le fichier, ou appuyez sur **Gérer** sous la liste **Applications favorites** ou **Documents favoris**. Si la barre **Gérer** n'est pas visible, appuyez sur le chevron (>) en regard d'**Applications favorites** ou de **Fichiers favoris**. 2 Appuyez sur la case à cocher en regard des noms de vos favoris dans les résultats de recherche ou dans la liste des applications ou des fichiers disponibles. Le favori que vous ajoutez en dernier s'affiche en haut de la liste des favoris.

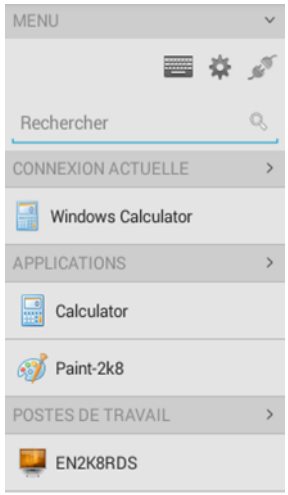
Tableau 3-3. Actions de la barre latérale Unity Touch pour un poste de travail distant (suite)

Action	Procédure
Supprimer une application ou un fichier de la liste des favoris	1 Recherchez l'application ou le fichier, ou appuyez sur **Gérer** sous la liste **Applications favorites** ou **Documents favoris**. Si la barre **Gérer** n'est pas visible, appuyez sur le chevron (>) en regard d'**Applications favorites** ou de **Documents favoris**. 2 Appuyez pour supprimer la coche en regard du nom de l'application ou du fichier dans la liste des favoris.
Réorganiser une application ou un fichier dans la liste des favoris	1 Appuyez sur **Gérer** sous la liste **Applications favorites** ou **Documents favoris**. Si la barre **Gérer** n'est pas visible, appuyez sur le chevron (>) en regard d'**Applications favorites** ou de **Documents favoris**. 2 Dans la liste des favoris, appuyez longuement sur la poignée à gauche du nom de l'application ou du fichier, et faites glisser le favori vers le haut ou vers le bas dans la liste.

Utilisation de la barre latérale Unity Touch avec une application distante

Vous pouvez accéder rapidement à une application distante à partir de la barre latérale Unity Touch. À partir de cette barre latérale, vous pouvez lancer des applications, basculer entre des applications en cours d'exécution, et réduire, agrandir, restaurer ou fermer des applications distantes. Vous pouvez également basculer vers un poste de travail distant.

Figure 3-2. Barre latérale Unity Touch pour une application distante



À partir de la barre latérale Unity Touch, vous pouvez effectuer de nombreuses actions sur une application distante.

Tableau 3-4. Actions de la barre latérale Unity Touch pour une application distante

Action	Procédure
Afficher ou masquer le clavier à l'écran	Appuyez sur l'icône **Clavier**.
Modifier des paramètres d'Horizon Client	Appuyez sur l'icône **Paramètres**.
Se déconnecter de l'application	Appuyez sur l'icône **Se déconnecter**.
Afficher la barre latérale	Faites glisser la barre latérale vers la droite ou appuyez sur l'onglet de la barre latérale. Lorsque la barre latérale est ouverte, vous ne pouvez pas effectuer d'actions sur la fenêtre de l'application.

Tableau 3-4. Actions de la barre latérale Unity Touch pour une application distante (suite)

Action	Procédure
Masquer la barre latérale	Faites glisser la barre latérale vers la gauche ou appuyez sur la zone de l'application. Lorsque la barre latérale est ouverte, vous ne pouvez pas effectuer d'actions sur la fenêtre de l'application.
Basculer entre des applications en cours d'exécution	Appuyez sur l'application sous **Connexion actuelle**.
Ouvrir une application	Appuyez sur le nom de l'application sous **Applications** dans la barre latérale. L'application démarre et la barre latérale se ferme.
Fermer une application en cours d'exécution	1 Appuyez longuement sur le nom de l'application sous **Connexion actuelle** jusqu'à ce que le menu contextuel s'affiche. 2 Appuyez sur **Fermer**.
Réduire une application en cours d'exécution	1 Appuyez longuement sur le nom de l'application sous **Connexion actuelle** jusqu'à ce que le menu contextuel s'affiche. 2 Appuyez sur **Réduire**.
Agrandir une application en cours d'exécution	1 Appuyez longuement sur le nom de l'application sous **Connexion actuelle** jusqu'à ce que le menu contextuel s'affiche. 2 Appuyez sur **Agrandir**.
Restaurer une application en cours d'exécution	1 Appuyez longuement sur le nom de l'application sous **Connexion actuelle** jusqu'à ce que le menu contextuel s'affiche. 2 Appuyez sur **Restaurer**.
Basculer vers un poste de travail distant	Appuyez sur le nom du poste de travail sous **Postes de travail**.

Utilisation du clavier à l'écran

Vous pouvez utiliser un clavier à l'écran dans une application ou un poste de travail distant. Pour afficher le clavier à l'écran, appuyez sur l'icône **Clavier** dans la barre latérale Unity Touch. Pour masquer le clavier à l'écran, appuyez de nouveau sur l'icône **Clavier**.

Le clavier à l'écran inclut les touches de navigation PageUp et PageDn, des touches de fonction et d'autres touches que vous utilisez souvent dans les environnements Windows, notamment Ctrl, Alt, Suppr, Maj, Win, Maj et Échap. Utilisez la touche Maj sur ce clavier lorsque vous devez utiliser des combinaisons de touches comprenant la touche Maj, telles que Ctrl+Maj. Pour effectuer une combinaison de ces touches, comme Ctrl+Alt+Maj, appuyez d'abord sur la touche Ctrl à l'écran. Une fois que la touche Ctrl est bleue, appuyez sur la touche Alt à l'écran. Une fois que la touche Alt est bleue, appuyez sur la touche Maj à l'écran. Une seule touche à l'écran est fournie pour la combinaison de touches Ctrl+Alt+Suppr.

Vous pouvez appuyer sur l'icône stylo à gauche de la touche Ctrl pour afficher la mémoire tampon d'entrée locale. Le texte que vous saisissez dans cette zone de texte n'est pas envoyé à une application tant que vous n'appuyez pas sur **Envoyer.** Par exemple, si vous ouvrez une application comme le Bloc-notes et que vous appuyez sur l'icône stylo, le texte que vous saisissez n'apparaît pas dans l'application Bloc-notes tant que vous n'appuyez pas sur **Envoyer**. Cette fonction est utile si votre connexion réseau est mauvaise et si les caractères n'apparaissent pas immédiatement lorsque vous les saisissez. Avec cette fonction, vous pouvez saisir rapidement jusqu'à 1 000 caractères, puis appuyer sur **Envoyer** ou sur **Retour** pour que les 1 000 caractères apparaissent en même temps dans l'application.

Résolutions d'écran et utilisation d'écrans externes

Vous pouvez utiliser Horizon Client avec des écrans externes et vous pouvez modifier les résolutions d'écran.

Lorsque vous branchez votre périphérique Chrome OS à un écran externe ou à un projecteur, vous pouvez afficher Horizon Client en mode plein écran en appuyant sur la touche Plein écran du clavier de votre périphérique.

Augmentation de la résolution d'écran pour un poste de travail distant

Par défaut, la résolution d'écran est définie pour afficher l'ensemble du poste de travail Windows sur le périphérique et les icônes du poste de travail et les icônes de la barre des tâches ont une certaine taille. Si vous augmentez la résolution, le poste de travail s'affiche toujours sur le périphérique, mais sa taille et celle des icônes de la barre des tâches sont plus petites.

Changement des paramètres de la résolution d'écran

Pour modifier le paramètre de résolution, appuyez sur l'icône **Paramètres** (engrenage) dans le coin supérieur droit de la fenêtre d'Horizon Client, appuyez sur **Affichage**, puis sur **Résolution**.

Utilisation de projecteurs

Vous pouvez utiliser le paramètre **Résolution** pour augmenter la résolution des projecteurs.

Utilisation de la fonctionnalité de prise en charge de plusieurs moniteurs

Avec la fonctionnalité de prise en charge de plusieurs moniteurs, vous pouvez étendre un poste de travail distant à l'aide d'un moniteur externe. Pour activer cette fonction, reportez-vous à la section « Activer la fonctionnalité de prise en charge de plusieurs moniteurs pour Horizon Client », page 12.

Utilisation de la fonctionnalité Audio/Vidéo en temps réel pour microphones

Avec la fonctionnalité Audio/Vidéo en temps réel, vous pouvez utiliser un microphone connecté à votre périphérique mobile sur votre poste de travail distant. L'Audio/Vidéo en temps réel est compatible avec des périphériques audio et des applications de conférence standard telles que Skype, WebEx et Google Hangouts.

L'Audio/Vidéo en temps réel est activé par défaut lorsque vous installez Horizon Client sur votre périphérique.

Remarque Seule la fonctionnalité d'entrée audio est prise en charge. La fonctionnalité de vidéo n'est pas prise en charge.

Pour plus d'informations sur la configuration de la fonctionnalité Audio/Vidéo en temps réel sur un poste de travail distant, consultez le document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

Enregistrement de documents dans une application distante

Vous pouvez créer et enregistrer des documents avec certaines applications distantes, telles que Microsoft Word ou WordPad. L'emplacement dans lequel vous enregistrez ces documents dépend de l'environnement réseau de votre société. Par exemple, vos documents peuvent être enregistrés sur un partage d'accueil de votre ordinateur local.

Les administrateurs peuvent utiliser un fichier de modèle ADMX pour définir une stratégie de groupe qui spécifie à quel endroit les documents sont enregistrés. Cette stratégie se nomme **Définir le répertoire de base de l'utilisateur des services Bureau à distance**. Pour plus d'informations, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

Internationalisation

L'interface utilisateur et la documentation sont disponibles en anglais, allemand, français, japonais, chinois simplifié, chinois traditionnel, coréen et espagnol. Vous pouvez également entrer des caractères dans ces langues.

Résolution des problèmes d' Horizon Client 4

Vous pouvez résoudre la plupart des problèmes d'Horizon Client en réinitialisant le poste de travail ou en réinstallant l'application.

Ce chapitre aborde les rubriques suivantes :

Redémarrer un poste de travail distant

Vous devrez peut-être redémarrer un poste de travail distant si le système d'exploitation du poste de travail cesse de répondre. 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 de poste de travail vous invite à 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 de poste de travail pour le poste de travail.

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 7* ou *Configuration d'applications et de postes de travail publiés dans Horizon 7*.

Prérequis

- Procurez-vous des informations d'identification de connexion, telles que le nom d'utilisateur et le mot de passe Active Directory, le nom d'utilisateur et le code secret RSA SecurID ou le nom d'utilisateur et le code secret pour l'authentification RADIUS.
- Si vous n'avez encore jamais ouvert de session, familiarisez-vous avec la procédure « Connexion à une application ou un poste de travail distant », page 18.

Procédure

1. Dans l'onglet **Serveurs**, appuyez sur le raccourci du serveur à connecter au serveur.
2. Si vous y êtes invité, entrez votre nom d'utilisateur et code secret RSA, votre nom d'utilisateur et mot de passe Active Directory, ou les deux.
3. Appuyez longuement sur le nom du poste de travail jusqu'à ce que le menu contextuel s'affiche.

   Vous pouvez effectuer cette étape à partir de l'onglet **Tout** ou **Favoris**.

4 Appuyez sur **Redémarrer** dans le menu contextuel.

Redémarrer est disponible uniquement si l'état du poste de travail est tel que l'action peut être effectuée.

Le système d'exploitation sur le poste de travail distant redémarre et Horizon Client se déconnecte et ferme la session sur le poste de travail.

Suivant

Il convient d'observer un temps d'attente suffisant pour le démarrage du système avant de tenter de se 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 un poste de travail distant ou des applications distantes », page 36.

Réinitialiser un poste de travail distant ou des applications distantes

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 des applications distantes ferme toutes les applications ouvertes.

La réinitialisation d'un poste de travail distant équivaut 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 distantes équivaut à quitter les applications sans enregistrer les données non enregistrées. Toutes les applications distantes ouvertes sont fermées, même les applications qui proviennent de batteries de serveurs RDS différentes.

Vous pouvez réinitialiser un poste de travail distant uniquement si un administrateur Horizon a activé la fonctionnalité de réinitialisation de poste de travail pour le poste de travail.

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 7* ou *Configuration d'applications et de postes de travail publiés dans Horizon 7*.

Prérequis

- Procurez-vous des informations d'identification de connexion, telles que le nom d'utilisateur et le mot de passe Active Directory, le nom d'utilisateur et le code secret RSA SecurID ou le nom d'utilisateur et le code secret pour l'authentification RADIUS.
- Si vous n'avez encore jamais ouvert de session, familiarisez-vous avec la procédure « Connexion à une application ou un poste de travail distant », page 18.

Procédure

1 Dans l'onglet **Serveurs**, appuyez sur le raccourci du serveur à connecter au serveur.

2 Si vous y êtes invité, entrez votre nom d'utilisateur et code secret RSA, votre nom d'utilisateur et mot de passe Active Directory, ou les deux.

3 Appuyez longuement sur le nom du poste de travail ou de l'application jusqu'à ce que le menu contextuel s'affiche.

Vous pouvez effectuer cette étape à partir de l'onglet **Tout** ou **Favoris**.

4 Appuyez sur **Réinitialiser** dans le menu contextuel.

Réinitialiser est disponible uniquement si l'état du poste de travail ou de l'application est tel que l'action peut être effectuée.

Lorsque vous réinitialisez un poste de travail distant, le système d'exploitation sur le poste de travail distant redémarre et Horizon Client se déconnecte et ferme la session sur le poste de travail. Lorsque vous réinitialisez des applications distantes, les applications se ferment.

Suivant

Il convient d'observer un temps d'attente suffisant pour le démarrage du système avant de tenter de se reconnecter à l'application ou au poste de travail distant.

Désinstaller Horizon Client

Il est parfois possible de résoudre certains problèmes avec Horizon Client en désinstallant et en réinstallant Horizon Client pour Chrome OS.

Vous désinstallez Horizon Client pour Chrome OS comme toute autre application Chrome OS.

Procédure

- Sur votre périphérique Chrome OS, appuyez sur l'icône Lanceur d'applications dans la barre des tâches, cliquez avec le bouton droit sur l'icône de l'application **Horizon Client pour Chrome OS** et sélectionnez **Désinstaller**.

Suivant

Réinstallez Horizon Client.

Reportez-vous à la section « Installer ou mettre à niveau Horizon Client pour Chrome OS », page 11.

Horizon Client cesse de répondre ou le poste de travail distant se fige

Lorsque la fenêtre se fige, essayez d'abord de réinitialiser le système d'exploitation du poste de travail distant.

Problème

Horizon Client ne fonctionne pas ou se ferme de façon répétée et inattendue, ou le poste de travail distant se bloque.

Cause

En partant du principe que les serveurs Horizon sont correctement configurés et que les ports corrects sont ouverts sur les pare-feu autour d'eux, les autres problèmes sont généralement liés à Horizon Client sur le périphérique ou au système d'exploitation invité sur le poste de travail distant.

Solution

- Si le système d'exploitation du poste de travail distant se fige, utilisez Horizon Client sur le périphérique pour réinitialiser le poste de travail.

  Cette option n'est disponible que si l'administrateur Horizon a activé cette fonctionnalité.
- Désinstallez et réinstallez l'application sur le périphérique.
- Si la réinitialisation du poste de travail distant et la réinstallation d'Horizon Client ne résolvent pas le problème, vous pouvez réinitialiser le périphérique Chrome OS, comme indiqué dans le guide de l'utilisateur du périphérique.
- Si vous obtenez une erreur de connexion lorsque vous tentez de vous connecter au serveur, vous devez peut-être modifier les paramètres proxy.

Problème lors de l'établissement d'une connexion en utilisant un proxy

Une erreur peut parfois se produire si vous essayez de vous connecter au Serveur de connexion à l'aide d'un proxy alors que vous êtes sur un réseau LAN.

Problème

Si l'environnement Horizon est configuré afin d'utiliser une connexion sécurisée à partir du poste de travail distant vers le Serveur de connexion, et si le périphérique client est configuré afin d'utiliser un proxy HTTP, vous risquez de ne pas pouvoir vous connecter.

Cause

Contrairement à Windows Internet Explorer, le périphérique client ne dispose pas d'une option Internet pour contourner le proxy pour les adresses locales. Lorsqu'un proxy HTTP est utilisé pour parcourir des adresses externes et que vous essayez de vous connecter au Serveur de connexion à l'aide d'une adresse interne, le message `Impossible d'établir une connexion` peut s'afficher.

Solution

- Supprimez les paramètres de proxy, afin que le périphérique n'utilise plus de proxy.

Index

S

V