Utilisation de VMware Horizon Client pour Windows 10 UWP

VMware Horizon Client for Windows 10 UWP 4.5

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

FR-002509-00

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 Windows 10 UWP

1

Utilisation de VMware Horizon Client pour Windows 10 UWP fournit des informations sur l'installation et l'utilisation du logiciel VMware Horizon® Client™ sur un périphérique Windows 10 pour se connecter à une application ou un poste de travail distant dans le centre de données.

Ces informations sont destinées aux administrateurs qui doivent configurer un déploiement d'Horizon comportant des périphériques clients Windows 10. Les informations sont rédigées pour des administrateurs système expérimentés qui connaissent parfaitement la technologie des machines virtuelles et les opérations de datacenter.

Configuration et installation 2

Lorsque vous configurez un déploiement d'Horizon pour des clients Windows 10 UWP, vous devez utiliser certains paramètres du Serveur de connexion, respecter la configuration système requise pour les serveurs Horizon et les clients des périphériques Windows 10 et installer l'application VMware Horizon Client Windows.

Ce chapitre aborde les rubriques suivantes :

Configuration système requise

Le périphérique sur lequel vous installez Horizon Client et tous les périphériques qu'il utilise doivent se conformer à une certaine configuration système.

Systèmes d'exploitation	■ Windows 10 Current Branch (CB) version 1703 (Creators Update) ■ Windows 10 Current Branch (CB) version 1607 (Anniversary Update) ■ Windows 10 Current Branch for Business (CBB) version 1607 (Anniversary Update) ■ Windows 10 Long-Term Servicing Branch (LTSB) version 1607 (Anniversary Update)
Authentification Windows Hello	Reportez-vous à la section « Configuration requise de l'authentification Windows Hello », page 8.

Serveur de connexion, serveur de sécurité et 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.
Protocole d'affichage pour applications et postes de travail distants	■ VMware Blast (requiert Horizon Agent 7.0 ou version ultérieure) ■ PCoIP

Configuration requise de l'authentification Windows Hello

Pour utiliser Windows Hello pour vous authentifier dans Horizon Client, vous devez respecter certaines conditions.

Modèles de périphériques Windows 10	Tout périphérique Windows 10 prenant en charge Windows Hello, tel que Microsoft Surface Pro 4.
Exigences de système d'exploitation	Configurez Windows Hello sous **Paramètres > Comptes > Options de connexion**.
Exigences du Serveur de connexion	■ Horizon 6 version 6.2 ou version ultérieure. ■ Activez l'authentification biométrique dans le Serveur de connexion. Pour plus d'informations, consultez « Configurer l'authentification biométrique » dans le document *Administration de View*.
Exigences d'Horizon Client	Activez Windows Hello en appuyant sur **Activer Windows Hello** dans la boîte de dialogue de connexion du serveur. Une fois que vous êtes connecté, vos informations d'identification Active Directory sont stockées en toute sécurité sur le périphérique Windows 10. **Activer Windows Hello** s'affiche la première fois que vous vous connectez et n'apparaît pas après que l'authentification Windows Hello est activée.

Vous pouvez utiliser l'authentification Windows Hello dans le cadre de l'authentification à deux facteurs avec l'authentification RSA SecurID et RADIUS.

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*.

- 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 utiliser l'authentification Windows Hello, vous devez activer l'authentification biométrique sur le Serveur de connexion. L'authentification biométrique est prise en charge dans Horizon 6 version 6.2 et ultérieures. Pour plus d'informations, reportez-vous au document *Administration de View*.

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 « Systèmes d'exploitation pris en charge pour Horizon Agent » dans le document *Installation de View*.

Installer ou mettre à niveau Horizon Client pour Windows 10 UWP

L'application VMware Horizon Client est une application Windows 10 UWP que vous installez comme les autres applications Windows 10 UWP.

Prérequis

- Vérifiez que votre périphérique client répond à la configuration système requise d'Horizon Client. Reportez-vous à la section « Configuration système requise », page 7.
- Si vous n'avez pas encore configuré le périphérique client, faites-le maintenant. Consultez le guide de l'utilisateur du fabricant de votre périphérique.

Procédure

1. Ouvrez l'application Microsoft Store sur votre périphérique et utilisez votre compte Microsoft pour vous connecter.
2. Recherchez l'application VMware Horizon Client.
3. Cliquez sur **Installer** ou **Libre** pour installer l'application VMware Horizon Client sur votre périphérique.

Enregistrer les informations sur les serveurs récents sur la fenêtre d'accueil d' Horizon Client

Vous pouvez configurer Horizon Client pour enregistrer un raccourci de serveur sur la fenêtre d'accueil après votre première connexion à un serveur.

Procédure

1 Appuyez sur le menu **Option** situé dans l'angle supérieur gauche de la barre de menus d'Horizon Client.

Si vous êtes connecté à un serveur, vous pouvez appuyer sur le menu **Option** dans le coin supérieur gauche de la fenêtre de sélection des postes de travail et des applications. Si vous êtes connecté à une application ou un poste de travail distant, vous pouvez appuyer sur le bouton **Option** dans la fenêtre du poste de travail ou de l'application et appuyer sur **Paramètres**.

2 Développez la section **Avancé** et appuyez pour basculer l'option **Enregistrer les informations sur les serveurs récents** sur **Activé**.

Si l'option est définie sur **Désactivé**, Horizon Client n'enregistre pas les serveurs récents sur la fenêtre d'accueil.

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 le menu **Option** dans le coin supérieur gauche de la barre de menus d'Horizon Client et développez la section **Options SSL**.

2 Pour activer ou désactiver un protocole de sécurité, appuyez sur le bouton bascule **Activé** ou **Désactivé** sous le nom du protocole de sécurité.

Vous pouvez activer et désactiver les protocoles TLSv1.0, TLSv1.1 et TLSv1.2. Les trois protocoles sont activés par défaut.

Remarque TLSv1.0 et TLSv1.2 requièrent que TLSv1.1 soit activé. Vous ne pouvez pas désactiver TLSv1.1 si TLSv1.0 et TLSv1.2 sont activés.

---

3 Pour modifier la chaîne de contrôle de chiffrement, remplacez la chaîne par défaut et appuyez sur **Modifier**.

4 (Facultatif) Si vous devez rétablir la chaîne de contrôle de chiffrement par défaut, appuyez sur **Par défaut**.

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

Configurer des options VMware Blast

Vous pouvez configurer des options de décodage H.264 et de condition réseau pour des sessions d'application et de poste de travail distant qui utilisent le protocole d'affichage VMware Blast.

Vous ne pouvez pas modifier l'option de condition réseau après vous être connecté à un serveur. Vous pouvez configurer le décodage H.264 avant ou après vous être connecté à un serveur.

Prérequis

Cette fonctionnalité requiert Horizon Agent 7.0 ou version ultérieure.

Procédure

1 Appuyez sur le menu **Option** dans le coin supérieur gauche de la barre de menus d'Horizon Client et développez la section **VMware Blast**.

Si vous êtes connecté à un serveur, vous pouvez appuyer sur le menu **Option** dans le coin supérieur gauche de la fenêtre de sélection des postes de travail et applications, développer la section **Protocole** et sélectionner **VMware Blast**. Vous ne pouvez pas modifier l'option de condition réseau après vous être connecté à un serveur.

2 Configurez les options de décodage et de condition réseau.

Option	Action
Autoriser le décodage H.264	Configurez cette option, avant ou après la connexion au Serveur de connexion, pour autoriser le décodage H.264 dans Horizon Client. 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. Désélectionnez cette option pour utiliser le décodage JPG/PNG.
Sélectionnez votre condition réseau pour une expérience optimale	Vous ne pouvez configurer cette option qu'avant la connexion au Serveur de connexion. Sélectionnez l'une des options de condition réseau suivantes : ■ **Excellent** : Horizon Client utilise uniquement la mise en réseau TCP. Cette option est idéale pour un environnement LAN. ■ **Classique (par défaut)** : Horizon Client fonctionne en mode mixte. En mode mixte, Horizon Client utilise la mise en réseau TCP lors de la connexion au serveur et utilise BEAT (Blast Extreme Adaptive Transport) si l'agent et Blast Security Gateway (si activé) prennent en charge la connectivité BEAT. Cette option est le paramètre par défaut. ■ **Faible** : Horizon Client n'utilise la mise en réseau BEAT que si le serveur tunnel BEAT est activé sur le serveur ; sinon il passe en mode mixte. **Remarque** Dans Horizon 7 versions 7.1 et antérieures, les instances du Serveur de connexion et du serveur de sécurité ne prennent pas en charge le serveur tunnel BEAT. Unified Access Gateway 2.9 et les versions ultérieures prennent en charge le serveur tunnel BEAT. Blast Security Gateway pour les instances du Serveur de connexion et du serveur de sécurité ne prend pas en charge la mise en réseau BEAT.

Affichage de l'aide pour Horizon Client

Pour accéder au système d'aide depuis l'application Horizon Client, appuyez sur le menu **Option** dans le coin supérieur gauche de la barre de menus, sur l'icône d'informations (**!**), puis sur le lien sous **Aide en ligne**. Vous pouvez également afficher le système d'aide une fois que vous êtes connecté à un serveur ou à une application ou un poste de travail distant.

Le système d'aide utilise les fonctions de votre navigateur Web, ainsi que certaines capacités supplémentaires, pour vous aider à accéder aux informations produit. Vous pouvez rechercher dans l'aide par le biais de requêtes contenant des guillemets, des caractères génériques et des opérateurs booléens.

Gestion des connexions aux applications et postes de travail distants 3

Vous pouvez utiliser Horizon Client pour vous connecter à un serveur et à des applications et des postes de travail distants.

En fonction de la façon dont un 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 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.

Si votre administrateur l'a autorisé, vous pouvez définir le mode de vérification des certificats. Dans la fenêtre d'accueil d'Horizon Client, appuyez sur le menu **Option** dans le coin supérieur gauche de la barre de menus et développez la section **Mode de vérification de certificat**. Vous disposez des choix suivants :

- **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.
- **Tenter de se connecter quels que soient les certificats d'identité du serveur**. Ce paramètre signifie qu'aucune vérification des certificats n'a lieu.

Comme le mécanisme de certificats utilisé dans les applications Windows 10 UWP est plus limité que pour les applications de bureau Windows, le contrôle de certification peut échouer même si le niveau est défini sur **Tenter de se connecter quels que soient les certificats d'identité du serveur**. Par exemple, le contrôle de certification peut échouer pour les raisons suivantes :

- Le certificat signé par l'autorité de certification racine a été révoqué.
- Le certificat signé par l'autorité de certification intermédiaire a été révoqué.
- Le certificat est valide, mais l'autorité de certification intermédiaire a été révoquée.
- Le certificat de la chaîne contient une extension inconnue qui est marquée « critique ».

Sélectionner un protocole d'affichage

Vous pouvez sélectionner le protocole d'affichage qu'Horizon Client utilise lorsque vous vous connectez à une application ou un poste de travail distant.

Procédure

1. Dans Horizon Client, appuyez sur le menu **Option** dans le coin supérieur gauche de la barre de menus d'Horizon Client.

   Si vous êtes connecté à un serveur, vous pouvez appuyer sur le menu **Option** dans le coin supérieur gauche de la fenêtre de sélection des postes de travail et des applications.

2. Développez la section **Protocole** et sélectionnez le protocole d'affichage à utiliser.

   VMware Blast requiert Horizon Agent 7.0 ou version ultérieure.

3. (Facultatif) Si vous avez sélectionné **VMware Blast**, activez ou désactivez le codage H.264 en appuyant et en basculant l'option **Autoriser le décodage H.264** sur **Activé** ou sur **Désactivé**.

   Lorsque cette option est définie sur **Activé**, Horizon Client autorise le codage H.264 si Horizon Agent pour l'application ou le poste de travail distant prend en charge le codage H.264. Si Horizon Agent pour l'application ou le poste de travail distant ne prend pas en charge le codage H.264, Horizon Client utilise le codage JPEG/PNG à la place. Lorsque cette option est définie sur **Désactivé** (paramètre par défaut), le codage H.264 n'est pas autorisé et Horizon Client utilise toujours le codage JPEG/PNG.

Lors de votre prochaine connexion à une application ou un poste de travail distant, Horizon Client utilise le protocole d'affichage que vous avez sélectionné. Vous ne pouvez pas modifier le protocole d'affichage pour une session actuellement connectée.

Si vous vous connectez à une application ou un poste de travail distant qui ne prend pas en charge le protocole d'affichage que vous avez sélectionné, Horizon Client affiche un message d'erreur.

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.

Pour utiliser les applications distantes, vous devez vous connecter au Serveur de connexion 6.0 ou version ultérieure.

Remarque Avant de laisser vos utilisateurs finaux accéder à leurs postes de travail distants, vérifiez que vous pouvez ouvrir une session sur un poste de travail distant à partir d'un périphérique client.

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.
- 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 », 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.

  Si votre entreprise possède un réseau interne sans fil afin de permettre un accès routable aux postes de travail distants et que votre périphérique peut utiliser ce réseau, vous n'avez pas besoin de mettre en place un serveur de sécurité ou une connexion 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.
- 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 13.
- Si vous prévoyez d'utiliser Windows Hello pour l'authentification, vérifiez que Windows Hello est configuré sur votre périphérique Windows 10. Pour plus d'informations sur les exigences, reportez-vous à « Configuration requise de l'authentification Windows Hello », page 8.

Procédure

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

2 Appuyez sur l'application **VMware Horizon Client**.

3 Connectez-vous à un serveur.

Option	Description
Se connecter à un nouveau serveur	Appuyez sur **Ajouter un serveur**, entrez le nom d'un serveur et appuyez sur **Se connecter**.
Se connecter à un serveur existant	Appuyez sur l'icône du serveur sur la fenêtre d'accueil.

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 vous êtes invité à entrer des informations d'identification RSA SecurID ou RADIUS, entrez le nom d'utilisateur et le mot de passe et appuyez sur **Connexion**.

Le code secret peut comporter un code PIN et le numéro généré sur le jeton.

5 Si vous êtes invité à fournir un nom d'utilisateur et un mot de passe, fournissez des informations d'identification Active Directory.

a Tapez le nom d'utilisateur et le mot de passe d'un utilisateur autorisé à utiliser au moins un pool de postes de travail ou d'applications.

b Sélectionnez un domaine.

c (Facultatif) Si le bouton **Activer Windows Hello** est disponible, cliquez dessus pour utiliser l'authentification Windows Hello.

Le bouton **Activer Windows Hello** est accessible uniquement si l'authentification biométrique est activée sur le serveur et que vous ne vous êtes pas authentifié auparavant avec Windows Hello.

d Appuyez sur **Ouverture de session**.

Si Windows Hello est activé et que vous vous connectez pour la première fois, vos informations d'identification Active Directory sont stockées en toute sécurité sur votre appareil Windows 10 pour une utilisation ultérieure.

6 Si vous êtes invité à fournir l'authentification Windows Hello, utilisez votre empreinte digitale, votre visage, votre iris ou votre code PIN pour vous authentifier.

Si vous ne souhaitez pas utiliser l'authentification Windows Hello, cliquez sur **Annuler** pour entrer un nom d'utilisateur et un mot de passe.

7 Appuyez sur un poste de travail ou une application pour vous y connecter.

L'application ou le poste de travail distant démarre.

Désactiver Windows Hello dans Horizon Client

Vous pouvez désactiver Windows Hello sur un serveur auquel vous vous étiez précédemment connecté avec l'authentification Windows Hello.

Prérequis

Vérifiez qu'un raccourci du serveur s'affiche dans la fenêtre d'accueil d'Horizon Client. Pour configurer Horizon Client de manière à enregistrer les raccourcis de serveur, reportez-vous à la section « Enregistrer les informations sur les serveurs récents sur la fenêtre d'accueil d'Horizon Client », page 10.

Procédure

1 Appuyez longuement sur le raccourci du serveur dans la fenêtre d'accueil d'Horizon Client.

2 Lorsque le menu contextuel s'affiche, appuyez sur **Se déconnecter du serveur**.

La prochaine fois que vous vous connecterez au serveur, vous pourrez entrer un nom d'utilisateur et un mot de passe, et le bouton **Activer Windows Hello** s'affichera dans la boîte de dialogue Connexion au serveur.

Épinglage d'une application ou d'un poste de travail distant à l'écran d'accueil

Pour épingler une application ou un poste de travail distant à l'écran d'accueil, il vous suffit de cliquer avec le bouton droit sur le poste de travail ou l'application dans la fenêtre de sélection de poste de travail et d'application, puis de sélectionner **Épingler à l'écran d'accueil** dans le menu contextuel.

Si vous n'êtes pas connecté au serveur lorsque vous appuyez sur l'application ou le poste de travail distant sur l'écran d'accueil, Horizon Client vous invite à vous authentifier sur le serveur avant de démarrer l'application ou le poste de travail distant. Si vous êtes déjà connecté au serveur, l'application ou le poste de travail distant démarre et vous n'avez pas besoin de vous authentifier sur le serveur.

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.

Lorsqu'une session est ouverte sur l'application ou le poste de travail distant, vous pouvez vous déconnecter en appuyant sur le bouton **Se déconnecter** dans la fenêtre du poste de travail ou de l'application et sur **Se déconnecter**.

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.

Fermeture de session sur un poste de travail distant

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.

Vous pouvez également fermer une session en appuyant sur le bouton **Ctrl+Alt+Suppr** dans la fenêtre de poste de travail ou d'application et en appuyant sur **Fermer la session**.

Tous les fichiers non enregistrés qui sont ouverts sur le poste de travail distant sont fermés lors de l'opération de fermeture de session. Si vous vous déconnectez d'un poste de travail distant sans fermer votre session, des applications restent ouvertes sur le poste de travail distant.

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

4

Horizon Client inclut des fonctionnalités communes aux autres applications de Windows 10 UWP, ainsi que des fonctionnalités spécifiques à des applications et des postes de travail distants.

Ce chapitre aborde les rubriques suivantes :

Matrice de prise en charge des fonctions

Certaines fonctionnalités sont prises en charge sur un type de client mais pas sur un autre. Par exemple, l'accès USB est pris en charge sur Horizon Client pour Windows, mais pas sur Horizon Client pour Windows 10 UWP.

Tableau 4-1. Fonctionnalités prises en charge sur les postes de travail Windows pour les Windows 10 UWP Horizon Clients

Fonction	Poste de travail Windows 10	Poste de travail Windows 8.x	Poste de travail Windows 7	Poste de travail Windows Vista	Poste de travail Windows XP	Postes de travail Windows Server 2008/2012 R2 et Windows Server 2016
redirection USB						
Audio/Vidéo en temps réel (RTAV)						
Redirection de port série						
Protocole d'affichage VMware Blast	X	X	X			X
Protocole d'affichage RDP						
Protocole d'affichage PCoIP	X	X	X	Limité	Limité	X
Gestion de persona						
Wyse MMR						
Redirection multimédia (MMR) Windows Media						
Impression basée sur l'emplacement	X	X	X	Limité	Limité	X
Impression virtuelle						
Cartes à puce						
RSA SecurID ou RADIUS	X	X	X	Limité	Limité	X
Authentification unique	X	X	X	Limité	Limité	X
Plusieurs écrans						

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, ou Horizon Agent 7.0 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 les services Bureau à distance Windows et Horizon Agent 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.

Le tableau suivant contient des lignes uniquement pour les fonctionnalités prises en charge. Certaines fonctionnalités sont prises en charge sur des hôtes RDS de machine virtuelle et pas sur des hôtes RDS de machine physique.

Tableau 4-2. Fonctionnalités prises en charge par les hôtes RDS avec View Agent 6.0.x ou version ultérieure, ou Horizon Agent 7.0 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 VMware Blast	Horizon Agent 7.0 et version ultérieure	Horizon Agent 7.0 et version ultérieure	Horizon Agent 7.0.2 et versions ultérieures
Protocole d'affichage PCoIP	X	X	Horizon Agent 7.0.2 et versions ultérieures
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)

Pour savoir quelles éditions de chaque système d'exploitation invité et quels Service Packs sont pris en charge, consultez la rubrique « Systèmes d'exploitation pris en charge pour View Agent » dans la documentation d'installation de View 5.x ou 6.x. Consultez « Systèmes d'exploitation pris en charge pour Horizon Agent » dans la documentation d'installation d'Horizon 7.

Utilisation du mode plein écran

Vous pouvez afficher des applications et des postes de travail distants en mode plein écran ou fenêtré sur un Surface Pro 4 ou Surface Book. Le mode plein écran est activé par défaut.

Pour basculer le mode plein écran, une fois connecté à une application ou un poste de travail distant, appuyez sur le bouton **Option** dans la fenêtre d'application ou de poste de travail distant et appuyez sur **Plein écran**.

Réglage de la résolution d'écran pour des applications et des postes de travail distants

Si votre tablette est dotée d'un écran haute résolution, il peut s'avérer difficile de déchiffrer les icônes et le texte sur une application ou un poste de travail distant. Vous pouvez réduire la résolution de l'écran pour améliorer la visibilité.

Pour modifier la résolution de l'écran avant de vous connecter à une application ou un poste de travail distant, appuyez sur le menu **Option** dans le coin supérieur gauche de la barre de menus Horizon Client, développez la section **Mode de résolution** et sélectionnez l'une des options de résolution.

Vous pouvez également modifier la résolution de l'écran une fois que vous êtes connecté à un serveur ou à une application ou un poste de travail distant.

Activer la fonctionnalité de zoom local

Lorsque vous activez la fonctionnalité de zoom local, vous pouvez resserrer ou écarter vos doigts sur votre écran tactile pour faire un zoom avant ou un zoom arrière de l'application ou du poste de travail distant.

Pour les postes de travail de machine virtuelle Windows 8 et Windows 10, et pour les postes de travail et les applications Windows Server 2012 R2 et Windows Server 2016 RDS, vous ne pouvez pas resserrer ou écarter vos doigts pour faire un zoom avant ou arrière sauf si vous activez la fonctionnalité de zoom local.

Procédure

1 Connectez-vous à une application ou un poste de travail distant.

2 Appuyez sur le bouton **Option** dans la fenêtre de poste de travail ou d'application et appuyez sur **Paramètres**.

3 Développez la section **Avancé** et appuyez pour basculer l'option **Zoom local** sur **Activé**.

Si l'option est définie sur **Désactivé**, vous ne pouvez pas utiliser la fonctionnalité de zoom local dans l'application ou le poste de travail distant. L'option est définie sur **Activé** par défaut.

Empêcher le verrouillage de l'écran

Après un certain temps d'inactivité, votre périphérique Windows 10 peut estomper l'affichage, activer l'écran de verrouillage ou éteindre l'écran pour économiser de l'énergie. Vous pouvez définir une option pour empêcher le verrouillage de l'écran pour une application ou un poste de travail distant.

Remarque Les périphériques Windows 10 enregistrent le visionnage et l'écoute comme faisant partie de la durée d'inactivité de l'utilisateur. La durée d'inactivité requise avant le verrouillage de l'écran dépend des paramètres d'utilisateur de votre périphérique.

Procédure

1 Connectez-vous à une application ou un poste de travail distant.

2 Appuyez sur le bouton **Option** dans la fenêtre de poste de travail ou d'application et appuyez sur **Paramètres**.

3 Développez la section **Avancé** et appuyez pour basculer l'option **Écran toujours allumé** sur **Activé**.

Si l'option est définie sur **Désactivé**, l'écran peut se verrouiller.

Utilisation de la barre latérale

Une fois que vous êtes connecté à une application ou un poste de travail distant, vous pouvez utiliser la barre latérale pour ouvrir d'autres postes de travail et applications.

Tableau 4-3. Actions de la barre latérale

Action	Description
Afficher la barre latérale	Appuyez sur le bouton **Option** dans la fenêtre d'application ou de poste de travail distant et appuyez sur **Barre latérale**.
Masquer la barre latérale	Appuyez n'importe où dans la fenêtre d'application ou de poste de travail distant.
Ouvrir une application ou un poste de travail distant	Appuyez sur le nom de l'application ou du poste de travail distant dans la barre latérale.
Rechercher une application ou un poste de travail distant	Entrez le nom de l'application ou du poste de travail distant dans la zone **Rechercher**. Pour ouvrir une application ou un poste de travail distant, appuyez sur son nom dans les résultats de la recherche.

Aides de mouvements et de navigation

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

Clic

Comme dans les autres applications, vous pouvez appuyer 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 :

- Utilisez une souris externe pour faire un clic droit.
- Sur un pavé tactile, appuyez avec deux doigts.
- Sur un écran tactile, appuyez et maintenez l'appui jusqu'à l'apparition du menu contextuel.

Zoom avant et arrière

Sur un écran tactile, resserrez ou écartez vos doigts pour zoomer.

Sur des systèmes d'exploitation prenant en charge l'entrée tactile, les zooms avant et arrière sur un écran tactile ne fonctionnent que si vous activez la fonctionnalité de zoom local. Reportez-vous à la section « Activer la fonctionnalité de zoom local », page 22. Windows 8, Windows 8.1, Windows 10, Windows Server 2012 et Windows Server 2016 prennent en charge l'entrée tactile.

Défilement et barres de défilement

Les options suivantes sont disponibles pour le défilement vertical :

- Utilisez une souris externe pour faire défiler.
- Sur un pavé tactile, appuyez et maintenez l'appui avec votre pouce, puis faites défiler vers le bas avec deux doigts.

- Sur un écran tactile, appuyez avec deux doigts et faites-les glisser pour faire défiler ou utilisez un doigt pour faire glisser la barre de défilement. Le texte sous vos doigts se déplace dans la même direction que vos doigts.

Son, musique et vidéo

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

Ctrl+Alt+Suppr

Comme la combinaison de touches Windows Ctrl+Alt+Suppr n'est pas prise en charge dans les applications et les postes de travail distants, appuyez sur le bouton **Ctrl+Alt+Suppr** dans la fenêtre de l'application ou du poste de travail distant à la place.

Multitâche

Vous pouvez basculer entre Horizon Client et d'autres applications sans perdre la connexion avec l'application ou le poste de travail distant.

Vous pouvez redimensionner l'application Horizon Client pour qu'elle s'affiche sur une partie de l'écran à côté d'une autre application.

Si vous laissez une session inactive pendant un certain temps, avant que la session n'expire, vous recevez une invite vous demandant si vous souhaitez maintenir la session active. Appuyez ou cliquez n'importe où sur l'écran ou appuyez sur une touche sur votre clavier pour maintenir la session active. Si un temps suffisamment long s'est écoulé pour que la connexion à l'application ou au poste de travail distant ait été perdue, Horizon Client revient à la fenêtre de sélection de postes de travail et d'applications et un message vous invite à vous reconnecter.

Utilisation d' Horizon Client avec une station d'accueil Microsoft Display Dock

L'application VMware Horizon Client fonctionne avec Continuum pour Windows 10 Mobile. Vous pouvez utiliser une station d'accueil Microsoft Display Dock pour connecter votre smartphone Windows 10 à un écran externe et une souris. Avec cette fonctionnalité, vous pouvez utiliser Horizon Client comme vous le feriez sur un ordinateur de bureau.

Copier et coller du texte et des images

Par défaut, vous pouvez copier-coller du texte à partir de votre système client vers une application ou un poste de travail distant. Si un administrateur Horizon active la fonctionnalité, vous pouvez également copier et coller du texte à partir d'une application ou d'un poste de travail distant vers votre système client ou entre deux applications ou postes de travail distants.

Vous pouvez uniquement copier et coller du texte brut. Les images et les données RTF (Rich Text Format) ne sont pas prises en charge.

Un administrateur Horizon peut définir cette fonctionnalité pour que les opérations Copier et Coller soient autorisées uniquement depuis votre système client vers une application ou un poste de travail distant ou uniquement depuis une application ou un poste de travail distant vers votre système client, ou les deux, ou aucun.

Les administrateurs Horizon configurent la capacité de copier et coller en configurant des paramètres de stratégie de groupe qui dépendent d'Horizon Agent. Selon la version d'Horizon Server et d'Horizon Agent utilisée, les administrateurs peuvent 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 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 7*.

Le Presse-papiers peut stocker 64 K de données pour des opérations Copier et Coller. Si vous tentez de copier plus que la taille maximale du Presse-papiers, le texte est tronqué.

Vous ne pouvez pas copier et coller des fichiers entre un poste de travail distant et le système de fichiers sur l'ordinateur client.

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 5

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

Vous pouvez également activer la collecte des journaux et envoyer les fichiers journaux à VMware pour dépannage.

Ce chapitre aborde les rubriques suivantes :

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 vous obtenez une erreur de connexion lorsque vous tentez de vous connecter au serveur, vous devez peut-être modifier les paramètres proxy.

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

Si vous êtes actuellement connecté à une application ou un poste de travail distant et qu'une session y est ouverte, vous pouvez appuyer sur le bouton **Se déconnecter** dans la fenêtre de poste de travail ou d'application et appuyer sur **Réinitialiser** pour réinitialiser l'application ou le poste de travail distant.

La commande **Réinitialiser** est disponible uniquement si l'administrateur Horizon l'a autorisée et uniquement si l'état de l'application ou du poste de travail distant permet l'exécution de l'action.

Vous devrez peut-être redémarrer une application ou un poste de travail distant si le système d'exploitation du poste de travail ou l'application cesse de répondre.

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'une application distante arrête toutes les applications distantes et ferme toutes vos sessions d'applications distantes. Les modifications non enregistrées dans les applications distantes peuvent être perdues.

Désinstaller l'application VMware Horizon Client

Vous pouvez parfois résoudre des problèmes avec Horizon Client en désinstallant et en réinstallant l'application VMware Horizon Client à partir du périphérique Windows 10 UWP.

Désinstallez Horizon Client comme vous le feriez pour n'importe quelle application Windows 10 UWP.

Procédure

1 Sur votre périphérique, recherchez l'application VMware Horizon Client.

2 Cliquez avec le bouton droit sur la vignette ou l'icône de **VMware Horizon Client** et appuyez sur **Désinstaller**.

Suivant

Réinstallez l'application VMware Horizon Client. Reportez-vous à la section « Installer ou mettre à niveau Horizon Client pour Windows 10 UWP », page 9.

Connexion à un serveur en mode Workspace ONE

Si vous ne pouvez pas vous connecter à un serveur directement via Horizon Client, ou si vos droits de poste de travail et d'application ne sont pas visibles dans Horizon Client, le mode Workspace ONE est peut-être activé sur le serveur.

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 via un raccourci ou un URI, 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 via Workspace ONE et qu'Horizon Client démarre, vous ne pouvez pas voir ou ouvrir d'autres applications ou postes de travail autorisés dans Horizon Client.

Cause

À partir d'Horizon 7 version 7.2, un administrateur 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 applications et postes de travail distants.

Collecter des journaux à envoyer au support technique

Vous pouvez activer la journalisation et collecter un lot de journaux à envoyer au support technique.

Pour résoudre certains problèmes, il peut vous être demandé de collecter des journaux à envoyer au support technique. La journalisation affectera les performances d'Horizon Client si une session de tunnel sécurisé est actuellement utilisée pour la connexion au poste de travail distant. Veillez à désactiver la fonction de journalisation avancée lorsque la journalisation n'est plus nécessaire.

Prérequis

Contactez le support technique de VMware pour savoir où vous devez envoyer les fichiers journaux que vous collectez.

Procédure

1 Dans Horizon Client, appuyez sur le menu **Option** situé dans le coin supérieur gauche de la barre de menus.

   Si vous êtes connecté à un serveur, vous pouvez appuyer sur le menu **Option** dans le coin supérieur gauche de la fenêtre de sélection des postes de travail et des applications. Si vous êtes connecté à une application ou un poste de travail distant, vous pouvez appuyer sur le bouton **Option** dans la fenêtre du poste de travail ou de l'application et appuyer sur **Paramètres**.

2 Développez la section **Journalisation** et appuyez pour basculer l'option **Activer la journalisation avancée** afin de l'activer.

3 Appuyez sur **Collecter des informations de support**, accédez à l'emplacement de votre périphérique pour stocker les fichiers journaux, sélectionnez le répertoire et appuyez sur **Choisir ce dossier**.

   Par exemple, pour simplifier les choses, vous pouvez appuyer sur l'élément **Poste de travail** pour enregistrer les journaux dans un dossier sur votre poste de travail local.

   Horizon Client crée un dossier nommé `vmware-view-logs-`*`timestamp`* à l'emplacement que vous avez spécifié.

4 (Facultatif) Pour créer un fichier `.zip` du dossier des journaux avant de l'envoyer au support technique, cliquez avec le bouton droit sur le dossier et sélectionnez **Envoyer vers > Dossier compressé**.

Suivant

Envoyez les journaux au support technique de VMware.

Index