# Guide d'installation et de configuration de VMware Horizon Client pour Windows 10 UWP

Septembre 2019

VMware Horizon Client for Windows 10 UWP 5.2

vmware®

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

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

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

docfeedback@vmware.com

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

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

# Table des matières

# Guide d'installation et de configuration de VMware Horizon Client pour Windows 10 UWP

1

Ce document, *Guide d'installation et de configuration de VMware Horizon Client pour Windows 10 UWP*, fournit des informations sur l'installation, la configuration et l'utilisation du logiciel VMware Horizon® Client™ sur un périphérique Windows 10.

Ces informations sont destinées aux administrateurs qui doivent configurer un déploiement d'Horizon comportant des périphériques clients Windows 10. Les informations sont destinées aux administrateurs système expérimentés qui connaissent bien le fonctionnement des centres de données et de la technologie des machines virtuelles.

Si vous êtes un utilisateur final, consultez le document *Guide de l'utilisateur de VMware Horizon Client pour Windows 10 UWP* sur Documentations de VMware ou affichez l'aide en ligne d'Horizon Client.

# Configuration et installation

2

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

Ce chapitre contient les rubriques suivantes :



## Configuration système requise pour les périphériques Windows 10

Le périphérique Windows 10 sur lequel vous installez l'application VMware Horizon Client et tous les périphériques qu'il utilise doivent se conformer à une certaine configuration système.

**Systèmes d'exploitation**

- Windows 10 1903 SAC
- Windows 10 1809 SAC
- Windows 10 1809 LTSC
- Windows 10 1607 LTSB

Parfois, les nouveaux systèmes d'exploitation Windows sont pris en charge après la publication de ce document. Pour obtenir les dernières

| | |
|---|---|
| | informations concernant la prise en charge des systèmes d'exploitation, consultez l'article 58096 de la base de connaissances de VMware. |
| **Authentification Windows Hello** | Reportez-vous à la section Configuration requise de l'authentification Windows Hello. |
| **Serveur de connexion, serveur de sécurité et View Agent ou Horizon Agent** | Dernière version de maintenance d'Horizon 6 version 6.2.x et versions ultérieures.<br>VMware recommande d'utiliser un serveur de sécurité ou un dispositif Unified Access Gateway pour que les périphériques clients ne nécessitent pas de connexion VPN. |
| **Protocoles d'affichage** | ■ VMware Blast (requiert Horizon Agent 7.0 ou version ultérieure)<br>■ PCoIP |

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

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

| | |
|---|---|
| **Postes de travail virtuels** | Pour utiliser la fonction Audio/Vidéo en temps réel avec des postes de travail virtuels, View Agent 6.2.x ou version ultérieure, ou Horizon Agent 7.0 ou version ultérieure, doit être installé.<br>Lorsque vous utilisez Microsoft Teams avec la fonctionnalité Audio/Vidéo en temps réel, VMware recommande que les postes de travail virtuels disposent d'au moins 4 vCPU et 4 Go de RAM. |
| **Postes de travail et applications publiés** | Pour utiliser la fonctionnalité Audio/Vidéo en temps réel avec des postes de travail et des applications publiés, Horizon Agent 7.0.2 ou version ultérieure doit être installé sur l'hôte RDS. |
| **Ordinateur Horizon Client ou périphérique d'accès client** | ■ La fonction Audio/Vidéo en temps réel est prise en charge par tous les systèmes d'exploitation client Windows qui utilisent Horizon Client pour Windows 10 UWP. Pour plus d'informations, reportez-vous à la section Configuration système requise pour les périphériques Windows 10. |

| | |
|---|---|
| | ■ Les pilotes des webcams et des périphériques audio doivent être installés, et la webcam ainsi que le périphérique audio doivent être opérationnels sur l'ordinateur client. Vous n'avez pas besoin d'installer les pilotes de périphérique sur la machine sur laquelle l'agent est installé. |
| **Protocoles d'affichage** | ■ VMware Blast (requiert Horizon Agent 7.0 ou version ultérieure) |

# 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.x ou version ultérieure.<br>■ Activez l'authentification biométrique dans le Serveur de connexion. Pour plus d'informations, consultez « Configurer l'authentification biométrique » dans le document *Administration d'Horizon 7*. |
| **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

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

## Unified Access Gateway et serveurs de sécurité

- Si votre déploiement Horizon inclut un dispositif Unified Access Gateway, configurez le Serveur de connexion pour qu'il fonctionne avec Unified Access Gateway. Reportez-vous au document *Déploiement et configuration d'Unified Access Gateway*. Les dispositifs Unified Access Gateway jouent le même rôle en tant que les serveurs de sécurité.
- Si votre déploiement d'Horizon inclut un serveur de sécurité, assurez-vous d'utiliser les dernières versions de maintenance du Serveur de connexion 6.2.x et du Serveur de sécurité 6.2.x ou versions ultérieures. Pour plus d'informations, reportez-vous au document d'installation de votre version d'Horizon.

## Pools de postes de travail et d'applications

- Vérifiez qu'un pool de postes de travail ou d'applications a été créé et que le compte d'utilisateur que vous souhaitez utiliser est autorisé à accéder au pool. Pour plus d'informations, consultez les documents *Configuration des postes de travail virtuels dans Horizon 7* et *Configuration d'applications et de postes de travail publiés dans Horizon 7*.

## Authentification des utilisateurs

- Pour utiliser l'authentification Windows Hello avec Horizon Client, vous devez activer l'authentification biométrique sur le Serveur de connexion. L'authentification biométrique est prise en charge dans Horizon 6 version 6.2.x et ultérieures. Pour plus d'informations, reportez-vous au document *Administration d'Horizon 7*.
- Pour utiliser l'authentification à deux facteurs, tels que l'authentification RSA SecurID ou RADIUS, avec Horizon Client, vous devez activer la fonctionnalité d'authentification à deux facteurs pour l'instance de Serveur de connexion. Pour plus d'informations, consultez les rubriques concernant l'authentification à deux facteurs dans le document *Administration d'Horizon 7*.
- Pour masquer l'URL du serveur dans Horizon Client, activez le paramètre global **Masquer les informations de serveur dans l'interface utilisateur client**. Ce paramètre est disponible dans Horizon 7 version 7.1 et version ultérieure. Pour plus d'informations, reportez-vous au document *Administration d'Horizon 7*.
- Pour masquer le menu déroulant **Domaine** dans Horizon Client, activez le paramètre global **Masquer la liste de domaines dans l'interface utilisateur client**. Ce paramètre est disponible dans Horizon 7 version 7.1 et version ultérieure. À partir d'Horizon 7 version 7.8, il est activé par défaut. Pour plus d'informations, reportez-vous au document *Administration d'Horizon 7*.
- Pour envoyer la liste de domaines à Horizon Client, activez le paramètre général **Envoyer la liste de domaines** dans Horizon Administrator. Ce paramètre est disponible dans Horizon 7 version 7.8 et versions ultérieures et est désactivé par défaut. Les versions antérieures d'Horizon 7 envoient la liste de domaines. Pour plus d'informations, reportez-vous au document *Administration d'Horizon 7*.

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

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

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

Les administrateurs Horizon 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 d'Horizon 7*.

# Installer ou mettre à niveau l'application VMware Horizon Client

L'application VMware Horizon Client est une application Windows 10 que vous installez de la même manière que les autres applications Windows 10.

### Conditions préalables

- Vérifiez que le périphérique client répond à la configuration système requise d'Horizon Client. Reportez-vous à la section Configuration système requise pour les périphériques Windows 10.

- Configurez le périphérique client Windows 10. Consultez le guide de l'utilisateur du fabricant du périphérique.

**Procédure**

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

# Enregistrer les informations sur les serveurs récents

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

**Procédure**

1. Ouvrez le menu **Option**.
   - Si vous n'êtes pas connecté à un serveur, 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, mais que vous n'êtes pas encore connecté à un poste de travail distant ou à une application publiée, appuyez sur le menu **Option** dans le coin supérieur gauche de la fenêtre de sélection de poste de travail ou d'application.
   - Si vous êtes connecté à un poste de travail distant ou à une application publiée, appuyez sur le bouton **Option** dans le menu flottant de la fenêtre du poste de travail ou de l'application publiée, puis appuyez sur **Paramètre**.
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 les options TLS avancées

Vous pouvez sélectionner les protocoles de sécurité et les algorithmes de chiffrement qu'Horizon utilise pour chiffrer les communications entre Horizon Client et les serveurs et entre Horizon Client et Horizon Agent.

Par défaut, TLS v1.1 et TLS v1.2 sont activés. SSL v2.0, SSL v3.0 et TLS v1.0 ne sont pas pris en charge. 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 le serveur auquel le système client se connecte, une erreur TLS se produit et la connexion échoue.

Pour plus d'informations sur la configuration des protocoles de sécurité que le serveur de connexion peut accepter, reportez-vous au document *Sécurité d'Horizon 7*.

### 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 TLS v1.1 et TLS v1.2. Les deux protocoles sont activés par défaut.
3. Pour modifier la chaîne de contrôle de chiffrement, remplacez la chaîne par défaut et appuyez sur **Modifier**.
4. (Facultatif) Pour 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 le décodage H.264 pour des sessions d'application publiée et de poste de travail distant qui utilisent le protocole d'affichage VMware Blast.

Vous pouvez configurer le décodage H.264 avant ou après vous être connecté à un serveur.

**Note** Dans les versions antérieures d'Horizon Client, vous deviez sélectionner une option de condition du réseau pour fournir la meilleure expérience utilisateur avec VMware Blast. Dans cette version, Horizon Client détecte les conditions du réseau actuelles et en choisit un transport pour fournir la meilleure expérience utilisateur automatiquement.

### Conditions préalables

Pour utiliser cette fonctionnalité, Horizon Agent 7.0 ou version ultérieure doit être installé.

### Procédure

1. Ouvrez le menu **Option**.
   - Si vous n'êtes pas connecté à un serveur, 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, développez la section **Protocole** et sélectionnez **VMware Blast**.
2. Pour activer ou désactiver le codage H.264, appuyez sur l'option **Autoriser le décodage H.264** et basculez-la sur **Activé** ou **Désactivé**.

   Lorsque cette option est définie sur **Activé** (par défaut), Horizon Client autorise le codage H.264 si l'instance d'Horizon Agent du poste de travail distant ou de l'application publiée prend en charge le

codage H.264. Si l'instance de Horizon Agent de l'application publiée ou du 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**, le codage H.264 n'est pas autorisé et Horizon Client utilise toujours le codage JPEG/PNG.

Les modifications du décodage H.264 seront appliquées la prochaine fois qu'un utilisateur se connectera à une application publiée ou un poste de travail distant et qu'il sélectionnera le protocole d'affichage VMware Blast. Vos modifications n'ont pas d'incidence sur les sessions VMware Blast existantes.

# Affichage de l'aide pour Horizon Client

Pour accéder à l'aide d'Horizon Client depuis l'application VMware Horizon Client, appuyez sur le menu **Option** dans le coin supérieur gauche de la barre de menus d'Horizon Client et appuyez sur l'icône d'informations (**!**), puis sur le lien sous **Aide en ligne**.

# Configurer le partage de données Horizon Client

Si votre administrateur Horizon a choisi de participer au programme d'amélioration du produit, VMware collecte et reçoit des données anonymes sur les systèmes clients afin de hiérarchiser la compatibilité matérielle et logicielle. Vous pouvez configurer si vous voulez partager des informations sur votre système client en activant ou en désactivant un paramètre dans Horizon Client.

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

### Procédure

1. Démarrez Horizon Client.
2. Appuyez sur le menu **Option** dans le coin supérieur gauche de la barre de menus d'Horizon Client et développez la section **Avancé**.
3. Développez la section **Autoriser le partage de données** et appuyez pour activer ou désactiver l'option **Autoriser le partage de données**.

## Données Horizon Client collectées par VMware

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

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

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

### Tableau 2-1. 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 :<br>■ i386<br>■ x86_64<br>■ arm |
| Nom du build du client | Non | Exemples :<br>■ VMware-Horizon-Client-Win32-Windows<br>■ VMware-Horizon-Client-Linux<br>■ VMware-Horizon-Client-iOS<br>■ VMware-Horizon-Client-Mac<br>■ VMware-Horizon-Client-Android<br>■ VMware-Horizon-Client-WinStore |
| Système d'exploitation hôte | Non | Exemples :<br>■ Windows 8.1<br>■ Windows 7, 64 bits Service Pack 1 (Build 7601)<br>■ iPhone OS 5.1.1 (9B206)<br>■ Ubuntu 12.04.4 LTS<br>■ Mac OS X 10.8.5 (12F45) |
| Noyau du système d'exploitation hôte | Non | Exemples :<br>■ Windows 6.1.7601 SP1<br>■ Darwin Kernel Version 11.0.0: Sun Apr 8 21:52:26 PDT 2012; root:xnu-1878.11.10~1/RELEASE_ARM_S5L8945X<br>■ Darwin 11.4.2<br>■ Linux 2.6.32-44-generic #98-Ubuntu SMP Mon Sep 24 17:27:10 UTC 2012<br>■ inconnu (pour Windows Store) |
| Architecture du système d'exploitation hôte | Non | Exemples :<br>■ x86_64<br>■ i386<br>■ armv71<br>■ ARM |

### Tableau 2-1. Données collectées depuis Horizon Client pour le programme d'amélioration du produit (suite)

| Description | Ce champ reste-t-il anonyme ? | Exemple |
|---|---|---|
| Modèle du système hôte | Non | Exemples :<br>■ Dell Inc. OptiPlex 960<br>■ iPad3,3<br>■ MacBookPro8,2<br>■ Dell Inc. Precision Workstation T3400 (A04 03/21/2008) |
| Processeur du système hôte | Non | Exemples :<br>■ Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GH<br>■ Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GH<br>■ 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 :<br>■ 4096<br>■ 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 :<br>■ Kingston<br>■ NEC<br>■ Nokia<br>■ Wacom |
| ID de produit de périphérique USB | Non | Exemples :<br>■ DataTraveler<br>■ Gamepad<br>■ Disque de stockage<br>■ Souris sans fil |
| Famille de périphériques USB | Non | Exemples :<br>■ Sécurité<br>■ Périphérique d'interface humaine<br>■ Imagerie |
| Nombre d'utilisations du périphérique USB | Non | (Nombre de partages du périphérique) |

# Gestion des connexions aux postes de travail distants et applications publiées

3

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

Les utilisateurs finaux peuvent être en mesure d'effectuer de nombreuses opérations sur les postes de travail distants, en fonction de la façon dont un administrateur Horizon configure les stratégies.

Ce chapitre contient les rubriques suivantes :



## Définition du mode de vérification des certificats dans Horizon Client

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

La vérification des certificats du serveur inclut les vérifications suivantes :

- Le certificat a-t-il été révoqué ?
- Le certificat a-t-il un autre but que de vérifier l'identité de l'expéditeur et de chiffrer les communications du serveur ? Autrement dit, s'agit-il du bon type de certificat ?

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

Pour définir le mode de vérification des certificats, démarrez Horizon Client, appuyez sur le menu **Option** dans le coin supérieur gauche de la barre de menus et développez la section **Mode de vérification des certificats**. Vous pouvez sélectionner l'une des options suivantes.

- **Ne jamais se connecter à des serveurs non autorisés**. Ce paramètre signifie que vous ne pouvez pas vous connecter au serveur si une des vérifications de certificat échoue. Un message d'erreur répertorie les vérifications qui ont échoué.
- **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 est plus limité que celui qui est utilisé par les applications de bureau Windows, la vérification des certificats peut échouer même si le niveau est défini sur **Tenter de se connecter quels que soient les certificats d'identité du serveur**. Par exemple, la vérification des certificats 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 ».

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

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

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

### Conditions préalables

- Procurez-vous 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.
- Si vous vous trouvez à l'extérieur du réseau de l'entreprise et que vous devez utiliser une connexion VPN pour accéder à des postes de travail distants ou à des applications publiées, vérifiez que le périphérique client est configuré pour utiliser une connexion VPN et activez la connexion.
- Vérifiez que vous disposez du nom de domaine complet (FQDN) du serveur qui fournit l'accès au poste de travail distant ou à l'application publiée. Les traits de soulignement (_) ne sont pas pris en charge dans les noms de serveur. Si le port n'est pas le port 443, vous avez également besoin du numéro de port.
- Configurez le mode de vérification des certificats pour le certificat présenté par le serveur. Reportez-vous à la section Définition du mode de vérification des certificats dans Horizon Client.
- Si vous prévoyez d'utiliser Windows Hello pour l'authentification, vérifiez que Windows Hello est configuré sur le périphérique Windows 10. Pour plus d'informations sur les exigences, reportez-vous à la section Configuration requise de l'authentification Windows Hello.

### 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 dans la fenêtre d'accueil. |

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

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 vos 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.

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

   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 le périphérique 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 (Facultatif) Pour sélectionner le protocole d'affichage à utiliser, appuyez sur le menu **Option** dans le coin supérieur gauche de la fenêtre de sélection des postes de travail et des applications et développez la section **Protocole**.

   **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.

8 Appuyez sur un poste de travail distant ou une application publiée pour vous y connecter.

Le poste de travail distant ou l'application publiée démarre.

# Désactiver l'authentification Windows Hello pour un serveur

Si vous vous êtes connecté précédemment à un serveur avec l'authentification Windows Hello, et que vous ne souhaitez plus utiliser l'authentification Windows Hello pour vous authentifier, vous devez désactiver l'authentification Windows Hello pour le serveur.

### Conditions préalables

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.

### Procédure

1. Appuyez longuement sur le raccourci du serveur dans la fenêtre d'accueil d'Horizon Client.
2. Pour désactiver l'authentification Windows Hello pour le serveur, appuyez sur **Se déconnecter du serveur** dans le menu contextuel.

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

Pour ajouter une vignette pour un poste de travail distant ou une application publiée à l'écran d'accueil sur le périphérique client, cliquez avec le bouton droit sur le poste de travail distant ou l'application publiée dans la fenêtre de sélection des postes de travail et applications, puis appuyez sur **Épingler au menu Démarrer** dans le menu contextuel.

Pour démarrer le poste de travail distant ou l'application publiée à partir de l'écran d'accueil, appuyez sur sa vignette. Si vous êtes déjà connecté au serveur, le poste de travail distant ou l'application publiée démarre immédiatement. Si vous n'êtes pas connecté au serveur, Horizon Client démarre et vous invite à vous authentifier sur le serveur avant de démarrer le poste de travail distant ou l'application publiée.

## Sélectionner une application publiée ou un poste de travail distant favori

Vous pouvez sélectionner comme favoris des postes de travail distants et des applications publiées. Une étoile identifie les éléments favoris dans la fenêtre de sélection des postes de travail et applications. Les éléments favoris sont enregistrés après que vous vous déconnectez du serveur.

### Conditions préalables

Connectez-vous au serveur.

### Procédure

- Pour sélectionner ou désélectionner un élément favori, cliquez avec le bouton droit sur un poste de travail distant ou une application publiée dans la fenêtre de sélection des postes de travail et applications 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 poste de travail distant ou de l'application publiée dans la fenêtre de sélection des postes de travail et applications.

- Pour désélectionner un élément favori, cliquez avec le bouton droit sur un poste de travail distant ou une application publiée dans la fenêtre de sélection des postes de travail et applications 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 poste de travail distant ou de l'application publiée dans la fenêtre de sélection des postes de travail et applications.

- Pour afficher uniquement les applications publiées ou les postes de travail distants favoris, appuyez sur le bouton **Afficher les favoris** (icône étoile) dans le coin supérieur droit de la fenêtre de sélection des postes de travail et applications.

  La fenêtre des favoris s'affiche. Pour revenir à la fenêtre de sélection des postes de travail et applications, appuyez sur le bouton **Tout afficher** dans le coin supérieur droit de la fenêtre des favoris.

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

Lorsque vous êtes connecté à un poste de travail distant, vous pouvez vous déconnecter sans fermer votre session afin que les applications restent ouvertes dans le poste de travail distant. Vous pouvez également vous déconnecter d'une application publiée de sorte que celle-ci reste ouverte.

Pour vous déconnecter d'un poste de travail distant ou d'une application publiée, appuyez sur le bouton **Se déconnecter** dans le menu flottant dans la fenêtre de l'application publiée ou du poste de travail distant, puis appuyez sur **Se déconnecter**.

**Note** Un administrateur Horizon peut configurer un poste de travail distant pour fermer la session lors de la déconnexion. Dans ce cas, toutes les applications ouvertes sur le poste de travail distant sont fermées.

# Fermeture de session sur un poste de travail distant

Si vous êtes 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 vous déconnecter en appuyant sur le bouton **Déconnecter** dans le menu flottant de la fenêtre du poste de travail distant, puis 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, les applications restent ouvertes sur le poste de travail distant.

# Déconnexion d'un serveur

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

Pour vous déconnecter d'un serveur, appuyez sur l'icône **Se déconnecter** dans le coin supérieur gauche de la fenêtre de sélection des postes de travail et des applications et appuyez sur **Fermer la session**.

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

4

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

Ce chapitre contient les rubriques suivantes :



## Matrice de prise en charge des fonctionnalités pour les clients Windows 10

Lorsque vous planifiez quels protocoles d'affichage et quelles fonctionnalités seront disponibles pour vos utilisateurs finaux, utilisez les informations suivantes pour déterminer quels systèmes d'exploitation invités prennent cette fonctionnalité en charge.

Tableau 4-1. Fonctionnalités prises en charge pour les postes de travail virtuels Windows

| Fonctionnalité | Poste de travail Windows 10 | Poste de travail Windows 8.x | Poste de travail Windows 7 | Poste de travail Windows Server 2008/2012 R2, Windows Server 2016 ou Windows Server 2019 |
|---|---|---|---|---|
| Redirection USB | | | | |
| Audio/Vidéo en temps réel (RTAV) | X | X | X | X |
| Redirection de port série | | | | |
| Protocole d'affichage VMware Blast | X | X | X | X |
| Protocole d'affichage RDP | | | | |
| Protocole d'affichage PCoIP | X | X | X | X |
| Gestion de persona | | | | |
| Redirection multimédia (MMR) Windows Media | | | | |
| Impression basée sur l'emplacement | X | X | X | X |
| Impression virtuelle | | | | |
| Redirection d'impression virtuelle VMware | | | | |
| Cartes à puce | | | | |
| RSA SecurID ou RADIUS | X | X | X | X |
| Authentification unique | X | X | X | X |
| Plusieurs écrans | | | | |

Les postes de travail distants Windows Server 2016 requièrent Horizon Agent 7.0.2 ou version ultérieure. Les postes de travail distants Windows Server 2019 requièrent Horizon Agent 7.7 ou version ultérieure.

Pour une description de ces fonctionnalités et de leurs limites, consultez le document *Planification de l'architecture Horizon 7*.

## 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 simultanées de poste de travail distant 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 pour les hôtes RDS**

| Fonctionnalité | Hôte RDS Windows Server 2008 R2 | Hôte RDS Windows Server 2012 R2 | Hôte RDS Windows Server 2016 | Hôte RDS Windows Server 2019 |
|---|---|---|---|---|
| RSA SecurID ou RADIUS | X | X | Horizon Agent 7.0.2 et versions ultérieures | Horizon Agent 7.7 et versions ultérieures |
| Authentification unique | X | X | Horizon Agent 7.0.2 et versions ultérieures | Horizon Agent 7.7 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 | Horizon Agent 7.7 et versions ultérieures |
| Protocole d'affichage PCoIP | X | X | Horizon Agent 7.0.2 et versions ultérieures | Horizon Agent 7.7 et versions ultérieures |
| Impression basée sur l'emplacement | View Agent 6.2.x à Horizon Agent 7.6 (machine virtuelle uniquement)<br>Horizon Agent 7.7 et versions ultérieures (machine virtuelle et machine physique) | View Agent 6.2.x à Horizon Agent 7.6 (machine virtuelle uniquement)<br>Horizon Agent 7.7 et versions ultérieures (machine virtuelle et machine physique) | Horizon Agent 7.0.2 à 7.6 (machine virtuelle uniquement)<br>Horizon Agent 7.7 et versions ultérieures (machine virtuelle et machine physique) | Horizon Agent 7.7 et versions ultérieures |

Pour plus d'informations sur les éditions de chaque système d'exploitation invité pris en charge, consultez la section « Systèmes d'exploitation pris en charge pour Horizon Agent » dans le document *Installation d'Horizon 7*.

# Utilisation du mode plein écran

Si vous utilisez un Surface Pro 4 ou un Surface Book, vous pouvez afficher les applications publiées et les postes de travail en mode plein écran ou fenêtré. Le mode plein écran est activé par défaut.

Après vous être connecté à un poste de travail distant ou à une application publiée, vous pouvez activer ou désactiver le mode plein écran en appuyant sur **Plein écran** dans le menu **Option** de la fenêtre de l'application publiée ou du poste de travail distant.

# Utilisation de la synchronisation DPI

La fonctionnalité de synchronisation DPI garantit que le paramètre DPI (points par pouce) d'un poste de travail distant ou d'une application publiée correspond au paramètre DPI de la machine cliente.

Pour ajuster manuellement la résolution, vous pouvez désactiver l'option **Autoriser la mise à l'échelle de l'affichage** dans Horizon Client et sélectionner une résolution. Pour plus d'informations, reportez-vous à la section Régler la résolution d'écran pour les postes de travail distants et les applications publiées.

Si la synchronisation DPI est désactivée, la mise à l'échelle de l'affichage est utilisée. La fonctionnalité de mise à l'échelle de l'affichage met le poste de travail distant ou l'application publiée à l'échelle appropriée.

Le paramètre de stratégie du groupe de l'agent **Synchronisation DPI** détermine si la fonctionnalité de synchronisation DPI est activée ou non. Cette fonctionnalité est activée par défaut. Grâce à la synchronisation DPI, la valeur DPI de la session distante change pour correspondre à la valeur DPI de la machine cliente lorsque vous vous connectez à un poste de travail distant ou à une application publiée. La fonctionnalité de synchronisation DPI requiert Horizon Agent 7.0.2 ou version ultérieure.

Si le paramètre de stratégie du groupe de l'agent **Synchronisation DPI par connexion** est activé, ainsi que le paramètre de stratégie de groupe **Synchronisation DPI**, l'option Synchronisation DPI est prise en charge lorsque vous vous reconnectez à un poste de travail distant. Cette fonctionnalité est désactivée par défaut. La fonctionnalité de synchronisation DPI par connexion requiert Horizon Agent 7.8 ou version ultérieure.

Pour plus d'informations sur les paramètres de stratégie de groupe **Synchronisation DPI** et **Synchronisation DPI par connexion**, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

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

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

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

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

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

- Windows 10 version 1607 et version ultérieure
- Windows Server 2016 et version ultérieure configuré en tant que poste de travail

La fonctionnalité de synchronisation DPI par connexion n'est pas prise en charge pour les postes de travail publiés ou les applications publiées.

Ci-dessous figurent les conseils d'utilisation de la fonctionnalité de synchronisation DPI.

- Si vous modifiez le paramètre DPI sur le système client, mais que le paramètre DPI ne change pas sur le poste de travail distant, vous aurez peut-être besoin de vous déconnecter et de vous reconnecter afin qu'Horizon Client détecte le nouveau paramètre DPI sur le système client.
- Si vous démarrez une session distante sur un système client avec un paramètre DPI supérieur à 100 % et que vous utilisez la même session sur un autre système client avec un paramètre DPI différent supérieur à 100 %, vous aurez peut-être besoin de vous déconnecter, puis de vous reconnecter sur le deuxième système client pour que la synchronisation DPI fonctionne sur le deuxième système client.
- Si un administrateur Horizon modifie la valeur du paramètre de stratégie de groupe **Synchronisation DPI** pour Horizon Agent, vous devez vous déconnecter, puis vous reconnecter, pour que le nouveau paramètre prenne effet.

# Régler la résolution d'écran pour les postes de travail distants et les applications publiées

Vous pouvez ajuster manuellement la résolution d'écran pour les postes de travail distants et les applications publiées.

**Note** Si l'écran du périphérique est petit ou si le DPI est de 100 %, utilisez le paramètre par défaut pour l'ajustement automatique au lieu d'ajuster la résolution d'écran manuellement.

### Procédure

1. Ouvrez le menu **Option**.
   - Si vous n'êtes pas connecté à un serveur, 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 mais que vous n'êtes pas encore connecté à un poste de travail distant ou une application publiée, appuyez sur le menu **Option** dans le coin supérieur gauche de la fenêtre de sélection de poste de travail ou d'application.
   - Si vous êtes connecté à un poste de travail distant ou une application publiée, appuyez sur le bouton **Option** dans le menu flottant et appuyez sur **Paramètre**.
2. Basculez l'option **Autoriser la mise à l'échelle de l'affichage** sur **Désactivé**.
3. Sélectionnez un mode de résolution.

# Configurer la fonctionnalité de zoom local

Avec la fonctionnalité de zoom local, vous pouvez rapprocher ou écarter vos doigts sur un écran tactile pour effectuer un zoom avant ou arrière à l'intérieur d'un poste de travail distant ou d'une application publiée.

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. Windows 8, Windows 8.1, Windows 10, Windows Server 2012 et Windows Server 2016 prennent en charge l'entrée tactile.

### Procédure

1. Connectez-vous à un poste de travail distant ou à une application publiée.
2. Appuyez sur le bouton **Option** dans le menu flottant de la fenêtre de l'application publiée ou du poste de travail distant, et appuyez sur **Paramètre**.
3. Développez la section **Avancé** et appuyez pour basculer l'option **Zoom local** sur **Activé** ou **Désactivé**.

# Empêcher le verrouillage de l'écran

Après un certain temps d'inactivité, le périphérique client 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 publiée ou un poste de travail distant.

**Note** 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 du périphérique.

### Procédure

1. Connectez-vous au poste de travail distant ou à l'application publiée.
2. Appuyez sur le bouton **Option** dans le menu flottant de la fenêtre de l'application publiée ou du poste de travail distant, et appuyez sur **Paramètre**.
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 publiée ou un poste de travail distant, vous pouvez utiliser la barre latérale pour ouvrir d'autres postes de travail distants et applications publiées.

**Tableau 4-3. Actions de la barre latérale**

| Action | Description |
|---|---|
| Afficher la barre latérale | Appuyez sur le bouton **Option** dans la fenêtre de l'application publiée ou du poste de travail distant et appuyez sur **Barre latérale**. |
| Masquer la barre latérale | Appuyez n'importe où dans la fenêtre de l'application publiée ou du poste de travail distant. |

**Tableau 4-3. Actions de la barre latérale (suite)**

| Action | Description |
| --- | --- |
| Ouvrir un poste de travail distant ou une application publiée | Appuyez sur le nom de l'application publiée ou du poste de travail distant dans la barre latérale.<br><br>**Note** Pour éviter de perdre des données, enregistrez-les avant de quitter une application publiée qui est en mode de sessions multiples. |
| Rechercher un poste de travail distant ou une application publiée | Entrez le nom de l'application publiée ou du poste de travail distant dans la zone **Rechercher**. Pour ouvrir l'application publiée ou le 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 Configurer la fonctionnalité de zoom local. 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.

## Utilisation de combinaisons de touches Windows

Après vous être connecté à une application ou un poste de travail distant, vous pouvez appuyer sur le bouton **Touche de combinaisons** dans le menu flottant pour utiliser les combinaisons de touches Windows suivantes :

- Ctrl+Alt+Suppr
- Win+R
- Alt+F4
- Alt

**Note** Win+R est disponible uniquement dans les sessions de postes de travail distants.

## 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.

# Multitâche

Vous pouvez basculer entre Horizon Client et d'autres applications sans perdre la connexion à un poste de travail distant ou une application publiée, et vous pouvez redimensionner l'application Horizon Client afin qu'elle occupe une partie de l'écran à côté d'une autre application.

Si vous laissez une session inactive pendant un certain temps, vous recevez une invite avant que la session n'expire, vous demandant si vous souhaitez maintenir la session active. Pour maintenir la session active, appuyez ou cliquez n'importe où sur l'écran ou appuyez sur une touche sur votre clavier. Si un temps suffisamment long s'est écoulé pour que la connexion à l'application publiée ou au poste de travail distant ait été perdue, Horizon Client revient à la fenêtre de sélection des postes de travail et applications et un message et 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 et coller à partir du système client vers un poste de travail distant ou une application publiée. Vous pouvez également copier et coller à partir d'un poste de travail distant ou d'une application publiée vers le système client, ou entre deux postes de travail distants ou applications publiées, si un administrateur Horizon active ces fonctionnalités.

Vous pouvez uniquement copier et coller du texte brut. Les images et le format RTF (Rich Text Format) ne sont pas pris en charge.

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

Un administrateur Horizon configure la possibilité de copier et coller en définissant des stratégies de groupe d'agent. Selon la version du serveur Horizon et de l'agent, un administrateur Horizon peut également avoir la possibilité d'utiliser des stratégies de groupe pour limiter les formats de Presse-papiers lors des opérations Copier et Coller, ou d'utiliser des stratégies de carte à puce pour contrôler le comportement de la fonctionnalité Copier-Coller sur les postes de travail distants. Pour plus d'informations, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

La fonctionnalité Copier-Coller présente les limites suivantes.

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

## Journalisation des activités copier et coller

Lorsque vous activez la fonctionnalité d'audit du Presse-papiers, Horizon Agent enregistre des informations sur les activités copier et coller dans un journal des événements sur la machine agent. La fonctionnalité d'audit du Presse-papiers est désactivée par défaut.

Pour activer la fonctionnalité d'audit du Presse-papiers, vous devez configurer le paramètre de stratégie de groupe **Configurer l'audit du Presse-papiers** pour VMware Blast ou PCoIP.

Vous pouvez éventuellement configurer le paramètre de stratégie de groupe **Bloquer la redirection du Presse-papiers du côté client lorsque le client ne prend pas en charge l'audit** pour VMware Blast ou PCoIP pour indiquer si vous voulez bloquer la redirection du Presse-papiers vers les clients qui ne prennent pas en charge la fonctionnalité d'audit du Presse-papiers.

Pour plus d'informations sur la configuration de ces paramètres de stratégie de groupe, consultez les rubriques « Paramètres de stratégie de VMware Blast » et « Paramètres de Presse-papiers PCoIP » dans le document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

Cette fonctionnalité requiert Horizon Agent 7.7 ou version ultérieure sur la machine agent.

Le journal des événements dans lequel sont enregistrées les informations sur les activités copier et coller se nomme VMware Horizon RX Audit. Pour afficher le journal des événements sur la machine agent, utilisez l'Observateur d'événements de Windows. Pour afficher le journal des événements dans un emplacement centralisé, configurez VMware Log Insight ou le Collecteur d'événements de Windows. Pour plus d'informations sur Log Insight, rendez-vous sur https://docs.vmware.com/fr/vRealize-Log-Insight/index.html. Pour plus d'informations sur le Collecteur d'événements Windows, reportez-vous à la documentation de Microsoft.

# Enregistrement de documents dans une application publiée

Vous pouvez créer et enregistrer des documents avec certaines applications publiées, 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.

Un administrateur Horizon peut utiliser le paramètre de stratégie de groupe des profils RDS appelé **Définir le répertoire de base des utilisateurs des services Bureau à distance** pour spécifier à quel emplacement les documents sont enregistrés. Pour plus d'informations, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

# Activer le mode de sessions multiples pour des applications publiées

Lorsque le mode de sessions·multiples est activé pour une application publiée, vous pouvez utiliser plusieurs sessions de la même application publiée lorsque vous vous connectez au serveur depuis différents périphériques clients.

Par exemple, si vous ouvrez une application publiée en mode de sessions·multiples sur le client A, puis que vous ouvrez la même application publiée sur le client B, elle reste ouverte sur le client A et une nouvelle session de l'application publiée s'ouvre sur le client B. En comparaison, lorsque le mode de sessions·multiples est désactivé (mode de session unique), la session de l'application publiée sur le client A se déconnecte et se reconnecte sur le client B.

La fonctionnalité de mode de sessions multiples présente les limites suivantes.

- Le mode de sessions multiples ne fonctionne pas pour les applications qui ne prennent pas en charge plusieurs instances, telles que Skype Entreprise.
- Si la session d'application est déconnectée lorsque vous utilisez une application publiée en mode de sessions multiples, vous êtes déconnecté automatiquement et les données non enregistrées sont perdues.

### Conditions préalables

Un administrateur Horizon doit activer le mode de sessions multiples pour le pool d'applications. Les utilisateurs ne peuvent pas modifier le mode de sessions multiples pour une application publiée, sauf si un administrateur Horizon l'autorise. Reportez-vous à *Configuration d'applications et de postes de travail publiés dans Horizon 7*. Cette fonctionnalité requiert Horizon 7 7.7 ou version ultérieure.

### Procédure

1. Connectez-vous à un serveur.
2. Appuyez sur le menu **Option** dans le coin supérieur gauche de la fenêtre de sélection des postes de travail et applications.
3. Développez la section **Avancé**, puis la section **Lancements multiples**.

   Si aucune application publiée n'est disponible pour une utilisation en mode de sessions multiples, l'option **Lancements multiples** n'apparaît pas.
4. Sélectionnez les applications publiées que vous voulez utiliser en mode de sessions multiples.

   Si un administrateur Horizon a appliqué le mode de sessions multiples pour une application publiée, vous ne pouvez pas modifier ce paramètre.

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

La fonctionnalité Audio/vidéo en temps réel vous permet d'utiliser une webcam ou un microphone du système client local sur un poste de travail distant ou une application publiée. La fonctionnalité Audio/vidéo en temps réel est compatible avec les applications de conférence standard et les applications vidéo basées sur navigateur. Elle prend en charge les webcams standards, les périphériques audio USB et l'entrée audio analogique.

Pour plus d'informations sur la configuration de la fonctionnalité Audio/Vidéo en temps réel sur la machine agent, y compris la configuration de la fréquence d'image et la résolution d'image, consultez le document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

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

Si un administrateur Horizon a configuré la fonctionnalité Audio/Vidéo en temps réel, vous pouvez utiliser une webcam intégrée ou connectée à l'ordinateur client dans un poste de travail distant ou une application publiée. Vous pouvez utiliser la webcam dans les applications de conférences telles que Skype, Webex ou Google Hangouts.

Lors de l'installation d'une application telle que Skype, Webex ou Google Hangouts sur un poste de travail distant, vous pouvez sélectionner des périphériques d'entrée et de sortie dans les menus de l'application.

Pour les postes de travail distants et les applications publiées, une webcam redirigée est nommée Webcam virtuelle VMware dans l'application.

Pour de nombreuses applications, vous n'avez pas à sélectionner un périphérique d'entrée.

Si plusieurs webcams sont connectées à l'ordinateur client local, vous pouvez configurer une webcam préférée à utiliser dans les sessions à distance.

Pour plus d'informations, consultez le document Sélectionner une webcam ou un microphone préféré sur un système client Windows 10 UWP.

## Sélectionner une webcam ou un microphone préféré sur un système client Windows 10 UWP

Avec la fonctionnalité audio/vidéo en temps réel, si plusieurs webcams ou microphones sont connectés au système client local, seul l'un des périphériques est utilisé sur l'application publiée ou le poste de travail distant. Pour spécifier la webcam ou le microphone préféré, vous devez configurer les paramètres audio/vidéo en temps réel dans Horizon Client.

Si il ou elle est disponible, la webcam ou le microphone préféré(e) est utilisé(e) sur le poste de travail distant ou l'application publiée. Si la webcam ou le microphone préféré(e) n'est pas disponible, une autre webcam ou un autre microphone est utilisé(e).

### Conditions préalables

Assurez-vous qu'une webcam USB ou un microphone USB ou d'un autre type est installé et opérationnel sur le système client.

### Procédure

1. Appuyez sur le menu **Option** situé dans l'angle supérieur gauche de la barre de menus d'Horizon Client.
2. Développez la section **Protocole** et sélectionnez **VMware Blast**.

   Les paramètres audio/vidéo en temps réel ne sont pas visibles, sauf si vous sélectionnez le protocole VMware Blast.
3. Pour sélectionner une webcam préférée, sélectionnez une webcam dans le menu déroulant **Webcam préférée**.
4. Pour sélectionner un microphone préféré, sélectionnez un microphone dans le menu déroulant **Microphone préféré**.

Lors du prochain démarrage d'une application publiée ou d'un poste de travail distant, le microphone ou la webcam préféré(e) que vous avez sélectionné(e) est redirigé(e) vers la session à distance.

# Internationalisation

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

# Dépannage de Horizon Client 5

Vous pouvez résoudre la plupart des problèmes avec Horizon Client en redémarrant ou en réinitialisant les postes de travail distants ou les applications publiées, ou en réinstallant Horizon Client.

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

Ce chapitre contient les rubriques suivantes :



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

Si un poste de travail distant ou une application publiée cesse de répondre, vous devrez le ou la réinitialiser.

La réinitialisation d'un poste de travail distant revient à appuyer sur le bouton **Réinitialiser** d'un ordinateur physique pour le forcer à redémarrer. Tous les fichiers ouverts sur le poste de travail distant sont fermés sans être enregistrés.

La réinitialisation d'une application publiée arrête toutes les applications publiées et ferme toutes les sessions d'application publiée. Les modifications non enregistrées dans les applications publiées peuvent être perdues.

Pour réinitialiser un poste de travail distant ou une application publiée, appuyez sur le bouton **Déconnecter** dans la fenêtre de l'application publiée ou du poste de travail distant et appuyez sur **Réinitialiser**.

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

# Désinstaller l'application VMware Horizon Client

Vous pouvez parfois résoudre des problèmes liés à Horizon Client en désinstallant et en réinstallant l'application VMware Horizon Client.

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

### Procédure

1 Sur le périphérique client, 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**.

### Étape suivante

Réinstallez l'application VMware Horizon Client. Reportez-vous à la section Installer ou mettre à niveau l'application VMware Horizon Client.

# Collecter des journaux à envoyer au support technique de VMware

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

Pour résoudre certains problèmes, il peut vous être demandé de collecter des fichiers journaux pour les envoyer au support technique de VMware. La journalisation pouvant affecter les performances de Horizon Client, désactivez la fonction de journalisation avancée lorsque la journalisation n'est plus nécessaire.

### Conditions préalables

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

### Procédure

1 Ouvrez le menu **Option**.

- Si vous n'êtes pas connecté à un serveur, 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 mais que vous n'êtes pas encore connecté à un poste de travail distant ou une application publiée, appuyez sur le menu **Option** dans le coin supérieur gauche de la fenêtre de sélection de poste de travail ou d'application.
- Si vous êtes connecté à un poste de travail distant ou une application publiée, appuyez sur le bouton **Option** dans le menu flottant de la fenêtre du poste de travail ou de l'application, puis appuyez sur **Paramètre**.

2 Développez la section **Journalisation** et appuyez pour basculer l'option **Activer la journalisation avancée** sur **Activé**.

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 de VMware, cliquez avec le bouton droit sur le dossier et sélectionnez **Envoyer vers > Dossier compressé**.

### Étape suivante

Envoyez les journaux au support technique de VMware.

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

Horizon Client cesse de répondre ou un poste de travail distant se fige.

### Problème

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

### Cause

Si le serveur est configuré correctement et que les ports corrects du pare-feu sont ouverts, la cause du problème concerne généralement Horizon Client sur le périphérique ou le système d'exploitation du poste de travail distant.

### Solution

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

  Cette option est disponible uniquement si un administrateur Horizon a activé la fonctionnalité de réinitialisation de poste de travail.
- Désinstallez et réinstallez l'application Horizon Client sur le périphérique client.
- Si vous obtenez une erreur de connexion lorsque vous tentez de vous connecter au serveur, vous devez peut-être modifier les paramètres du proxy.

# Connexion à un serveur en mode Workspace ONE

Vous ne pouvez pas vous connecter à un serveur directement via Horizon Client ou votre poste de travail distant, et les droits d’accès à l’application publiée ne sont pas visibles dans Horizon Client.

### Problème

- Lorsque vous tentez de vous connecter au serveur directement via Horizon Client, Horizon Client vous redirige vers le portail Workspace ONE.
- Lorsque vous ouvrez un poste de travail ou une application publiée via un URI ou un raccourci, ou lorsque vous ouvrez un fichier local via l'association de fichier, la demande vous redirige vers le portail Workspace ONE pour l'authentification.
- Lorsque vous ouvrez un poste de travail ou une application publiée via Workspace ONE et que Horizon Client démarre, vous ne pouvez pas voir ou ouvrir d'autres applications publiées ou postes de travail autorisés dans Horizon Client.

### Cause

À partir d'Horizon 7 version 7.2, un administrateur Horizon peut activer le mode Workspace ONE sur une instance du Serveur de connexion. Ce comportement est normal lorsque le mode Workspace ONE est activé sur une instance du Serveur de connexion.

### Solution

Utilisez Workspace ONE pour vous connecter à un serveur compatible avec Workspace ONE et accéder à vos postes de travail distants et à vos applications publiées.