Administration du plug-in View Agent Direct-Connection

Décembre 2019
VMware Horizon 7 7.11

vmware®

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

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

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

docfeedback@vmware.com

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

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

Table des matières

Administration du plug-in View Agent Direct-Connection

Administration du plug-in View Agent Direct-Connection fournit des informations sur l'installation et la configuration du plug-in View Agent Direct-Connection. Ce plug-in est une extension installable d'Horizon Agent qui permet à Horizon Client de se connecter directement à un poste de travail basé sur une machine virtuelle, à un poste de travail publié ou à une application sans utiliser le Serveur de connexion Horizon. Toutes les fonctionnalités de poste de travail ou d'application s'exécutent de la même manière que lorsque l'utilisateur se connecte via le Serveur de connexion.

Public cible

Ces informations sont destinées à un administrateur qui souhaite installer, mettre à niveau ou configurer le plug-in View Agent Direct-Connection sur un poste de travail basé sur une machine virtuelle ou sur un hôte RDS. Ce guide a été rédigé à l'attention des administrateurs système Windows expérimentés qui connaissent bien la technologie de machines virtuelles et les opérations de centre de données.

Installation du plug-in View Agent Direct-Connection 1

Le plug-in VADC (View Agent Direct-Connection) autorise les clients Horizon Client à se connecter directement aux postes de travail basés sur une machine virtuelle, aux postes de travail publiés ou aux applications. Le plug-in VADC, qui est une extension de Horizon 7 Agent, est installé sur des postes de travail basés sur une machine virtuelle ou des hôtes RDS.

Ce chapitre contient les rubriques suivantes :

Configuration système requise pour le plug-in View Agent Direct-Connection

Le plug-in View Agent Direct-Connection (VADC) est installé sur des machines sur lesquelles Horizon 7 Agent est déjà installé. Pour obtenir la liste des systèmes d'exploitation qu'Horizon 7 Agent prend en charge, reportez-vous à la section « Systèmes d'exploitation pris en charge pour Horizon Agent » dans le document *Installation d'Horizon 7*.

Le plug-in VADC a les exigences supplémentaires suivantes :

- La machine virtuelle ou physique sur laquelle le plug-in VADC est installé doit disposer d'au moins 128 Mo de mémoire RAM vidéo pour garantir le bon fonctionnement.
- Pour une machine virtuelle, vous devez installer VMware Tools avant d'installer Horizon 7 Agent.
- Une machine physique prend en charge Windows 10 Entreprise version 1803 ou 1809.

Le protocole de prise en charge du plug-in VADC est le suivant :

- Une machine virtuelle sur laquelle le plug-in VADC est installé prend en charge les protocoles Blast et PCoIP.

- Une machine physique sur laquelle le plug-in VADC est installé ne prend en charge que le protocole Blast.

Note Un poste de travail basé sur une machine virtuelle qui prend en charge VADC peut joindre un domaine Microsoft Active Directory ou peut être membre d'un groupe de travail.

Installer le plug-in View Agent Direct-Connection

Le plug-in View Agent Direct-Connection (VADC) est modularisé dans un fichier de programme d'installation Windows que vous pouvez télécharger à partir du site Web VMware et installer.

Conditions préalables

- Vérifiez que Horizon 7 Agent n'est pas installé. Si votre environnement n'inclut pas le Serveur de connexion Horizon 7, installez Horizon 7 Agent à partir de la ligne de commande et spécifiez un paramètre qui demande à Horizon 7 Agent de ne pas s'enregistrer dans le Serveur de connexion Horizon 7. Reportez-vous à la section Installer Horizon 7 Agent pour HTML Access.
- Activez le paramètre DMA d'écran pour les machines virtuelles sur vSphere 6.0 et versions ultérieures. Si le DMA d'écran est désactivé, les utilisateurs voient un écran noir lorsqu'ils se connectent au poste de travail distant. Pour plus d'informations sur la configuration du DMA d'écran, consultez l'article 2144475 de la base de connaissances de VMware http://kb.vmware.com/kb/2144475.

Procédure

1. Téléchargez le fichier du programme d'installation du plug-in VADC à partir de la page de téléchargement VMware à l'adresse http://www.vmware.com/go/downloadview.

   Le nom de fichier du programme d'installation est VMware-viewagent-direct-connection-x86_64-y.y.y-xxxxxx.exe pour Windows 64 bits ou VMware-viewagent-direct-connection--y.y.y-xxxxxx.exe pour Windows 32 bits, où y.y.y est le numéro de version et xxxxxx le numéro de build.
2. Double-cliquez sur le fichier du programme d'installation.
3. (Facultatif) Modifiez le numéro de port TCP.

   Le numéro de port par défaut est 443.
4. (Facultatif) Choisissez comment configurer le service Pare-feu Windows.

   Par défaut, l'option **Configurer automatiquement le Pare-feu Windows** est cochée et le programme d'installation configure le Pare-feu Windows afin d'autoriser les connexions réseau requises.

5 (Facultatif) Indiquez si vous souhaitez désactiver SSL 3.0.

Par défaut, l'option **Désactiver automatiquement la prise en charge de SSLv3 (recommandé)** est sélectionnée et le programme d'installation désactive SSL 3.0 au niveau du système d'exploitation. Cette option ne s'affiche pas et le programme d'installation n'exécute aucune action si SSL 3.0 est déjà activé ou désactivé de manière explicite dans le registre. Si cette option est décochée, le programme d'installation n'exécute pas cette action.

6 Suivez les invites et terminez l'installation.

Installer le plug-in View Agent Direct-Connection en silence

Vous pouvez utiliser la fonctionnalité d'installation silencieuse de MSI (Microsoft Windows Installer) pour installer le plug-in View Agent Direct-Connection (VADC). Lors d'une installation silencieuse, vous utilisez la ligne de commande sans avoir besoin de répondre aux invites de l'assistant.

Avec l'installation silencieuse, vous pouvez déployer efficacement le plug-in VADC dans une grande entreprise. Pour plus d'informations sur Windows Installer, reportez-vous à la section « Options de ligne de commande de Microsoft Windows Installer » dans le document *Configuration des postes de travail virtuels dans Horizon 7*. Le plug-in VADC prend en charge les propriétés MSI suivantes.

Tableau 1-1. Propriétés MSI pour l'installation silencieuse du plug-in View Agent Direct-Connection

Propriété MSI	Description	Valeur par défaut
LISTENPORT	Port TCP utilisé par le plug-in VADC pour accepter les connexions à distance. Par défaut, le programme d'installation configurera le pare-feu Windows pour qu'il autorise le trafic sur le port.	443
MODIFYFIREWALL	Si cette propriété est définie sur 1, le programme d'installation configurera le pare-feu Windows pour qu'il autorise le trafic sur LISTENPORT. Si elle est définie sur 0, le programme d'installation ne le configurera pas.	1
DISABLE_SSLV3	Si SSL 3.0 est déjà activé ou désactivé explicitement dans le registre, le programme d'installation ignore cette propriété. Sinon, le programme d'installation désactive SSL 3.0 au niveau du système d'exploitation si cette propriété est définie sur 1 et n'exécute aucune action si cette propriété est définie sur 0.	1

Conditions préalables

- Vérifiez que Horizon Agent n'est pas installé. Si votre environnement n'inclut pas le Serveur de connexion Horizon, installez Horizon Agent à partir de la ligne de commande et spécifiez un paramètre qui demande à Horizon Agent de ne pas s'enregistrer sur le Serveur de connexion Horizon. Reportez-vous à la section Installer Horizon 7 Agent pour HTML Access.

Procédure

1 Ouvrez une invite de commande Windows.

2 Exécutez le fichier d'installation du plug-in VADC avec les options de la ligne de commande pour spécifier une installation silencieuse. Vous pouvez éventuellement spécifier des propriétés MSI facultatives.

L'exemple suivant installe le plug-in VADC avec les options par défaut.

```
VMware-viewagent-direct-connection--y.y.y-xxxxxx.exe /s
```

L'exemple suivant installe le plug-in VADC et spécifie un port TCP que vadc écoutera pour des connexions à distance.

```
VMware-viewagent-direct-connection--y.y.y-xxxxxx.exe /s /v"/qn LISTENPORT=9999"
```

Configuration avancée du plug-in View Agent Direct-Connection 2

Vous pouvez utiliser les paramètres de configuration par défaut du plug-in View Agent Direct-Connection ou les personnaliser via les objets de stratégie de groupe (GPO) de Windows Active Directory ou en modifiant des paramètres de Registre Windows spécifiques.

Ce chapitre contient les rubriques suivantes :

Paramètres de configuration du plug-in View Agent Direct-Connection

Le fichier de modèle d'administration ADMX pour la configuration de VMware View Agent (`view_agent_direct_connection.admx`) contient les paramètres de stratégie relatifs au plug-in View Agent Direct-Connection.

Les paramètres de configuration de View Agent Direct-Connection se trouvent dans l'Éditeur de gestion de stratégie de groupe dans **Configuration ordinateur > Modèles d'administration > Configuration de VMware View Agent > Configuration de View Agent Direct-Connection**.

Tableau 2-1. Paramètres de configuration du plug-in View Agent Direct-Connection

Paramètre	Description
Applications activées	Ce paramètre prend en charge le lancement de l'application sur les hôtes de session Bureau à distance. Le paramètre par défaut est activé.
Paires de valeurs de nom de configuration du client	Liste de valeurs à transmettre au client sous la forme nom=valeur. Par exemple : clientCredentialCacheTimeout=1440.

Tableau 2-1. Paramètres de configuration du plug-in View Agent Direct-Connection (suite)

Paramètre	Description
Délai d'expiration de la mise en cache des informations d'identification du client	Délai, en minutes, pendant lequel un client Horizon autorise un utilisateur à utiliser un mot de passe enregistré. 0 correspond à Jamais, -1 correspond à Toujours. Horizon Client donne aux utilisateurs la possibilité d'enregistrer leur mot de passe si ce paramètre est défini sur une valeur valide. La valeur par défaut est 0 (jamais).
Délai d'expiration de la session client	Durée maximale en secondes pendant laquelle une session est conservée active si un client n'est pas connecté. La valeur par défaut est de 36 000 secondes (10 heures).
Paramètre client : AlwaysConnect	La valeur peut être définie sur `TRUE` ou `FALSE`. Le paramètre AlwaysConnect est envoyé à Horizon Client. Si cette stratégie est définie sur `TRUE`, elle remplace toutes les préférences client enregistrées. Aucune valeur n'est définie par défaut. L'activation de cette stratégie définit la valeur sur `TRUE`. La désactivation de cette stratégie définit la valeur sur `FALSE`.
Paramètre client : AutoConnect	Ce paramètre remplace les préférences enregistrées d'Horizon Client. Aucune valeur n'est définie par défaut. L'activation de cette stratégie définit la valeur sur true, sa désactivation définit la valeur sur false.
Paramètre client : ScreenSize	Paramètre ScreenSize envoyé à Horizon Client. S'il est activé, il remplace les préférences enregistrées du client. S'il n'est ni configuré ni désactivé, les préférences du client sont utilisées.
Protocole par défaut	Protocole d'affichage par défaut utilisé par Horizon Client pour se connecter au poste de travail. Si aucune valeur n'est définie, la valeur par défaut est BLAST.
Clause d'exclusion de responsabilité activée	La valeur peut être définie sur `TRUE` ou `FALSE`. Si elle est définie sur `TRUE`, le texte d'exclusion de responsabilité que l'utilisateur doit accepter à l'ouverture de session s'affiche. Il correspond au « Texte d'exclusion de responsabilité » si celui-ci a été rédigé, ou il est extrait du GPO `Configuration\Paramètres Windows\Paramètres de sécurité\Stratégies locales\Options de sécurité : Ouverture de session interactive`. Le paramètre par défaut pour disclaimerEnabled est `FALSE`.
Texte d'exclusion de responsabilité	Texte d'exclusion de responsabilité qui s'affiche pour les utilisateurs d'Horizon Client à l'ouverture de session. La stratégie Exclusion de responsabilité activée doit être définie sur `TRUE`. Si le texte n'est pas spécifié, la valeur par défaut utilisée est celle de la stratégie Windows `Configuration\Paramètres Windows\Paramètres de sécurité \Stratégies locales\Options de sécurité`.
Port Blast externe	Numéro de port envoyé à Horizon Client pour le numéro de port TCP de destination utilisé avec le protocole HTML5/Blast. Le signe + devant le numéro indique un nombre relatif calculé par rapport au numéro de port utilisé pour HTTPS. Ne définissez cette valeur que si le numéro de port exposé en externe ne correspond pas au port sur lequel le service écoute. En général, ce numéro de port s'utilise dans un environnement NAT. Aucune valeur n'est définie par défaut.
Port Framework Channel externe	Numéro de port envoyé à Horizon Client pour le numéro de port TCP de destination utilisé avec le protocole Framework Channel. Le signe + devant le numéro indique un nombre relatif calculé par rapport au numéro de port utilisé pour HTTPS. Ne définissez cette valeur que si le numéro de port exposé en externe ne correspond pas au port sur lequel le service écoute. En général, ce numéro de port s'utilise dans un environnement NAT. Aucune valeur n'est définie par défaut.
Adresse IP externe	Adresse IPv4 envoyée à Horizon Client pour l'adresse IP de destination utilisée avec les protocoles secondaires (RDP, PCoIP, Framework Channel, etc.). Ne définissez cette valeur que si l'adresse exposée en externe ne correspond pas à celle de la machine de poste de travail. En général, cette adresse s'utilise dans un environnement NAT. Aucune valeur n'est définie par défaut.

Tableau 2-1. Paramètres de configuration du plug-in View Agent Direct-Connection (suite)

Paramètre	Description
Port PCoIP externe	Numéro de port envoyé à Horizon Client pour le numéro de port TCP/UDP de destination utilisé avec le protocole PCoIP. Le signe + devant le numéro indique un nombre relatif calculé par rapport au numéro de port utilisé pour HTTPS. Ne définissez cette valeur que si le numéro de port exposé en externe ne correspond pas au port sur lequel le service écoute. En général, ce numéro de port s'utilise dans un environnement NAT. Aucune valeur n'est définie par défaut.
Port RDP externe	Numéro de port envoyé à Horizon Client pour le numéro de port TCP de destination utilisé avec le protocole RDP. Le signe + devant le numéro indique un nombre relatif calculé par rapport au numéro de port utilisé pour HTTPS. Ne définissez cette valeur que si le numéro de port exposé en externe ne correspond pas au port sur lequel le service écoute. En général, ce numéro de port s'utilise dans un environnement NAT. Aucune valeur n'est définie par défaut.
Numéro de port HTTPS	Port TCP sur lequel le plug-in écoute les demandes HTTPS entrantes provenant d'Horizon Client. Si vous modifiez cette valeur, vous devez effectuer la modification correspondante dans le Pare-feu Windows pour autoriser le trafic entrant. La valeur par défaut est 443.
Redirection multimédia (MMR) activée	Détermine si MMR est activé pour les systèmes client. MMR est un filtre de Microsoft DirectShow qui permet de transférer des données multimédia de codecs spécifiques sur des postes de travail Horizon au système client directement via un socket TCP. Les données sont ensuite directement décodées sur le système client, lorsqu'elles sont lues. La valeur par défaut est désactivée. MMR ne fonctionne pas correctement si le matériel d'affichage vidéo du système client ne prend pas en charge la superposition. Les systèmes clients peuvent ne pas contenir suffisamment de ressources pour gérer le décodage multimédia local.
Réinitialisation activée	La valeur peut être définie sur `TRUE` ou `FALSE`. Lorsque ce paramètre est défini sur `TRUE`, Horizon Client authentifié peut effectuer un redémarrage au niveau du système d'exploitation. Le paramètre par défaut est désactivé (`FALSE`).
Délai d'expiration de session	Période pendant laquelle un utilisateur peut garder une session ouverte avec Horizon Client. La valeur est définie en minutes. La valeur par défaut est de 600 minutes. Lorsque le délai arrive à expiration, toutes les sessions de poste de travail et d'applications de l'utilisateur sont déconnectées.
Connexion USB automatique	La valeur peut être définie sur `TRUE` ou `FALSE`. Connecte des périphériques USB au poste de travail lorsqu'ils sont branchés. Si cette stratégie est définie, elle remplace les préférences client enregistrées. Aucune valeur n'est définie par défaut.
USB activé	La valeur peut être définie sur `TRUE` ou `FALSE`. Détermine si des postes de travail peuvent utiliser des périphériques USB connectés au système client. La valeur par défaut est activée. Pour empêcher l'utilisation de périphériques externes pour des raisons de sécurité, désactivez le paramètre (`FALSE`).
Délai d'inactivité de l'utilisateur	En l'absence d'activité utilisateur sur Horizon Client pendant ce délai, les sessions de poste de travail et d'application de l'utilisateur sont déconnectées. La valeur est définie en secondes. La valeur par défaut est de 900 secondes (15 minutes).

Tableau 2-1. Paramètres de configuration du plug-in View Agent Direct-Connection (suite)

Paramètre	Description
Authentification par certificat X509	Détermine si l'authentification par certificat X.509 de carte à puce est désactivée, autorisée ou requise.
Authentification par certificat SSL X509 activée	Détermine si l'authentification par certificat X.509 de carte à puce est activée via une connexion SSL directe depuis Horizon Client. Cette option n'est pas requise si l'authentification par certificat X.509 est gérée via un point de terminaison SSL intermédiaire. La modification de ce paramètre nécessite un redémarrage d'Horizon Agent.

Les numéros de ports externes et les valeurs d'adresses IP externes sont utilisés pour prendre en charge la traduction d'adresses réseau (Network Address Translation, NAT) et le mappage des ports. Pour plus d'informations, reportez-vous à Utilisation de la traduction d'adresses réseau et du mappage de ports

Pour l'authentification par carte à puce, l'autorité de certification (CA) qui signe les certificats de carte à puce doit exister dans le magasin de certificats Windows. Pour obtenir des informations sur l'ajout d'une autorité de certification, reportez-vous à Ajouter une autorité de certification à un magasin de certificats Windows.

Note Si un utilisateur tente de se connecter à l'aide d'une carte à puce à une machine Windows 7 ou Windows Server 2008 R2 et que le certificat de la carte à puce a été signé par une autorité de certification intermédiaire, la tentative peut échouer, car Windows peut envoyer au client une liste d'émetteurs approuvés ne contenant pas les noms des autorités de certification intermédiaires. Le cas échéant, le client n'est pas en mesure de sélectionner un certificat de carte à puce correspondant. Pour éviter ce problème, définissez la valeur de registre `SendTrustedIssuerList` (REG_DWORD) sur 0 dans la clé de registre `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL`. Lorsque cette valeur de registre est définie sur 0, Windows n'envoie pas de liste d'émetteurs approuvés au client qui peut alors sélectionner tous les certificats valides de la carte à puce.

Désactivation des chiffrements faibles dans les protocoles SSL/TLS

Pour atteindre une meilleure sécurité, vous pouvez configurer l'objet de stratégie de groupe (GPO) de stratégie de domaine pour garantir que les communications qui utilisent le protocole SSL/TLS entre des Horizon Client et des postes de travail basés sur une machine virtuelle ou des hôtes RDS n'autorisent pas les chiffrements faibles.

Procédure

1. Sur le serveur Active Directory, modifiez les objets de stratégie de groupe (GPO) en sélectionnant **Démarrer > Outils d'administration > Gestion de stratégie de groupe**, puis en cliquant avec le bouton droit sur GPO et en sélectionnant **Édition**.
2. Dans l'éditeur de la gestion des stratégies du groupe accédez à **Configuration de l'ordinateur > Stratégies > Modèles d'administration > Réseau > Paramètres de configuration SSL**.
3. Double-cliquez sur **Ordre des suites de chiffrement SSL**.

4 Dans la fenêtre Ordre des suites de chiffrement SSL cliquez sur **Activé**.

5 Dans le volet Options, remplacez la totalité du contenu du champ Suites de chiffrement SSL avec la liste de chiffrement suivante :

```
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384,
TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHA
```

Les suites de chiffrement sont répertoriées ci-dessus sur des lignes distinctes pour plus de clarté. Lorsque vous collez la liste dans le champ de texte, les suites de chiffrement doivent être sur une même ligne, sans espaces après les virgules.

6 Quittez l'éditeur de la gestion des règles du groupe.

7 Redémarrez les machines VADC pour que la nouvelle stratégie de groupe prenne effet.

Note Si Horizon Client n'est pas configuré pour prendre en charge un chiffrement pris en charge par le système d'exploitation du poste de travail virtuel, la négociation TLS/SSL échoue et le client ne peut plus se connecter.

Pour plus d'informations sur la configuration des suites de chiffrement prises en charge dans les clients Horizon Client, reportez-vous à la documentation Horizon Client à l'adresse https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

Remplacement du certificat de serveur TLS auto-signé par défaut

Un certificat de serveur TLS auto-signé ne peut pas fournir à Horizon Client une protection suffisante contre les menaces de falsification et d'écoute. Pour protéger vos postes de travail contre ces menaces, vous devez remplacer le certificat auto-signé généré.

Lorsque le plug-in View Agent Direct-Connection démarre pour la première fois après l'installation, il génère automatiquement un certificat de serveur TLS auto-signé et le place dans le magasin de certificats de Windows. Le certificat de serveur TLS est présenté à Horizon Client pendant la négociation du protocole TLS pour fournir au client des informations sur ce poste de travail. Ce certificat de serveur TLS auto-signé par défaut ne peut pas fournir de garanties sur ce poste de travail, il doit être remplacé par un certificat signé par une autorité de certification qui est approuvé par le client et est entièrement validé par les vérifications de certificat d'Horizon Client.

La procédure de stockage de ce certificat dans le magasin de certificats Windows et la procédure de remplacement par un certificat signé par une autorité de certification appropriée sont les mêmes que celles utilisées pour le Serveur de connexion Horizon 7. Pour plus d'informations sur cette procédure de remplacement de certificat, reportez-vous à « Configuration de certificats TLS pour les serveurs Horizon 7 » dans le document *Installation d'Horizon 7*.

Les certificats disposant d'une extension Autre nom de l'objet (SAN) et de certificats génériques sont pris en charge.

Note Pour distribuer les certificats de serveur TLS signés par une autorité de certification à un grand nombre de postes de travail à l'aide du plug-in View Agent Direct-Connection, utilisez la stratégie d'inscription à Active Directory pour distribuer les certificats à chaque machine virtuelle. Pour plus d'informations, reportez-vous à http://technet.microsoft.com/en-us/library/cc732625.aspx.

Autoriser Horizon Client à accéder aux postes de travail et aux applications

Le mécanisme d'autorisation permettant à un utilisateur d'accéder directement aux postes de travail et aux applications est géré au sein d'un groupe du système d'exploitation local appelé **Utilisateurs de View Agent Direct-Connection**.

Si un utilisateur est membre de ce groupe, il est autorisé à se connecter au poste de travail basé sur une machine virtuelle, à un poste de travail publié ou à des applications publiées. Lorsque le plug-in est installé pour la première fois, ce groupe local est créé et contient le groupe Utilisateurs authentifiés. Tous les utilisateurs authentifiés par le plug-in sont autorisés à accéder au poste de travail ou aux applications.

Pour restreindre l'accès à ce poste de travail ou à cet hôte RDS, vous pouvez modifier l'appartenance à ce groupe et spécifier une liste d'utilisateurs et de groupes d'utilisateurs. Ces utilisateurs peuvent être locaux ou être des utilisateurs et des groupes d'utilisateurs du domaine. Si l'utilisateur ne fait pas partie de ce groupe, il reçoit un message après l'authentification lui signalant qu'il n'est pas autorisé à accéder à ce poste de travail basé sur une machine virtuelle ou aux applications ou au poste de travail publié hébergés sur cet hôte RDS.

Utilisation de la traduction d'adresses réseau et du mappage de ports

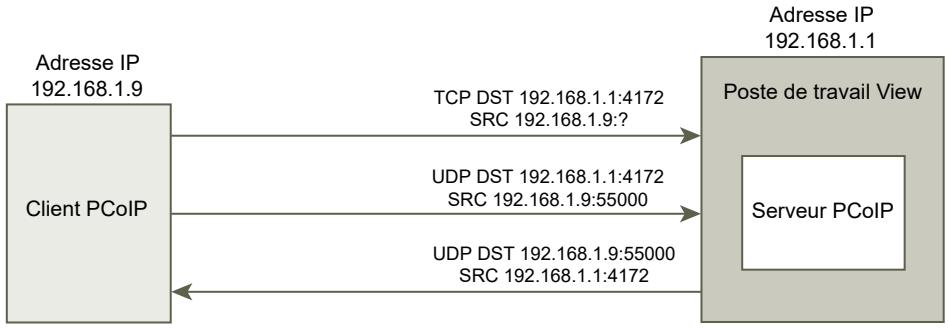
La traduction d'adresses réseau (NAT) et la configuration du mappage de ports sont requises si Horizon Client se connecte à des postes de travail de machine virtuelle sur différents réseaux.

Dans les exemples du présent document, vous devez configurer les informations d'adressage externe sur le poste de travail afin qu'Horizon Client puisse les utiliser pour se connecter au poste de travail à l'aide d'un périphérique de traduction d'adresses réseau ou de mappage de ports. Cette URL est la même que celle des paramètres URL externe et URL externe PCoIP sur le Serveur de connexion Horizon 7 et le serveur de sécurité.

Si Horizon Client se trouve sur un autre réseau et que le périphérique NAT est situé entre Horizon Client et le poste de travail exécutant le plug-in, une traduction d'adresses réseau ou une configuration du mappage de ports est requise. Par exemple, si un pare-feu est situé entre Horizon Client et le poste de travail, le pare-feu agit comme un périphérique de traduction d'adresses réseau ou de mappage de ports.

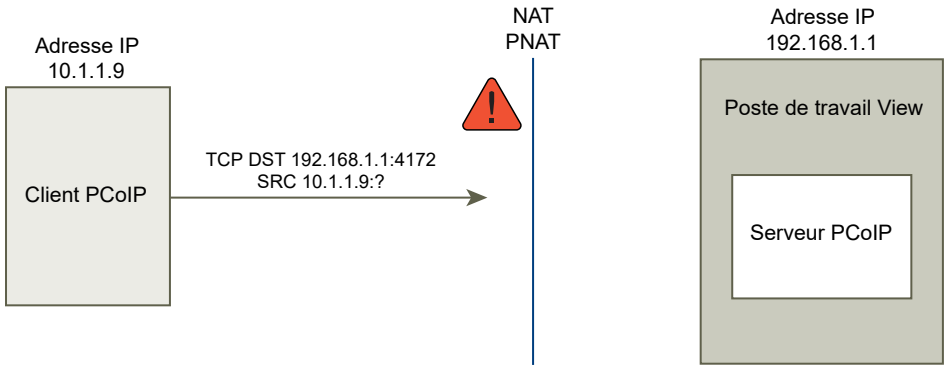
Un exemple de déploiement d'un poste de travail dont l'adresse IP est 192.168.1.1 illustre la configuration de la traduction d'adresses réseau et du mappage de ports. Un système Horizon Client disposant de l'adresse IP 192.168.1.9 sur le même réseau établit une connexion PCoIP en utilisant TCP et UDP. Cette connexion est directe, sans traduction d'adresses réseau ni configuration du mappage de ports.

Figure 2-1. PCoIP direct à partir d'un client sur le même réseau



Si vous ajoutez un périphérique NAT entre le client et le poste de travail pour qu'ils fonctionnent dans un espace d'adressage différent et si vous ne modifiez pas la configuration dans le plug-in, les paquets PCoIP ne seront pas correctement acheminés et échoueront. Dans cet exemple, le client utilise un espace d'adresses différent et dispose de l'adresse IP 10.1.1.9. Cette installation échoue, car le client utilisera l'adresse du poste de travail pour envoyer les paquets PCoIP TCP et UDP. L'adresse de destination 192.168.1.1 ne fonctionnera pas à partir du réseau du client et peut provoquer l'affichage d'un écran vide sur le client.

Figure 2-2. PCoIP à partir d'un client via un périphérique NAT montrant la panne

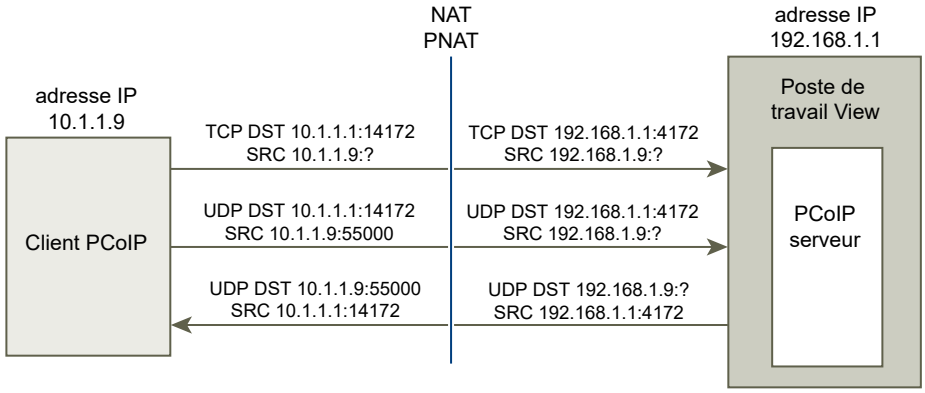


Pour résoudre ce problème, vous devez configurer le plug-in pour utiliser une adresse IP externe. Si `externalIPAddress` est configuré sur 10.1.1.1 pour ce poste de travail, le plug-in attribue au client l'adresse IP 10.1.1.1 lors de l'établissement de connexions du protocole de poste de travail au poste de travail. Pour PCoIP, le service PCoIP Secure Gateway doit être démarré sur le poste de travail pour cette configuration.

Pour le mappage de ports, lorsque le poste de travail utilise le port PCoIP standard 4172, alors que le client doit utiliser un port de destination différent, mappé au port 4172 sur le périphérique de mappage de ports, vous devez configurer le plug-in pour cette installation. Si le périphérique de mappage de ports mappe le port 14172 à 4172, le client doit utiliser le port de destination 14172 pour PCoIP. Vous devez configurer cette installation pour PCoIP. Définissez `externalPCoIPPort` dans le plug-in sur 14172.

Dans une configuration qui utilise la traduction d'adresses réseau et le mappage de ports, `externalIPAdress` est défini sur 10.1.1.1, qui est traduit en 192.168.1.1, et `externalPColPPort` est défini sur 14172, qui fait l'objet d'un mappage de port à 4172.

Figure 2-3. PCoIP à partir d'un client via un périphérique NAT et un mappage de ports



Comme pour la configuration de ports PCoIP TCP/UDP externes pour PCoIP, si le port RDP (3389) ou le port Framework Channel (32111) fait l'objet d'un mappage de ports, vous devez configurer `externalRDPPort` et `externalFrameworkChannelPort` pour spécifier les numéros de ports TCP que le client utilisera pour établir ces connexions au moyen d'un périphérique de mappage de ports.

Schéma d'adressage avancé

Lorsque vous configurez des postes de travail basés sur une machine virtuelle pour qu'ils soient accessibles via un périphérique de traduction d'adresses réseau et de mappage de ports sur la même adresse IP externe, vous devez attribuer à chaque poste de travail un ensemble unique de numéros de port. Les clients peuvent ensuite utiliser la même adresse IP de destination, mais utilisent un numéro de port TCP unique pour la connexion HTTPS pour diriger la connexion vers un poste de travail virtuel spécifique.

Par exemple, le port HTTPS 1000 dirige les demandes vers un poste de travail, le port HTTPS 1005 vers un autre poste, tous deux utilisant la même adresse IP de destination. Dans ce cas, la configuration de numéros de port externes uniques pour chaque poste de travail pour les connexions de protocole de postes de travail serait trop complexe. Pour cette raison, les paramètres de plug-in `externalPCoIPPort`,`externalRDPPort` et `externalFrameworkChannelPort` peuvent prendre une expression relationnelle facultative plutôt qu'une valeur statique pour définir un numéro de port relatif au numéro de port HTTPS de base utilisé par le client.

Si le périphérique de mappage de ports utilise le numéro de port 1000 pour HTTPS, mappé à TCP 443, le numéro port 1001 pour RDP, mappé à TCP 3389, le numéro de port 1002 pour PCoIP, mappé à TCP et UDP 4172, et le numéro de port 1003 pour le canal d'infrastructure, mappé à TCP 32111, pour simplifier la configuration, les numéros de port externes peuvent être configurés de la manière suivante :`externalRDPPort=+1`, `externalPCoIPPort=+2` et `externalFrameworkChannelPort=+3`. Lorsque la connexion HTTPS provient d'un client qui a utilisé le numéro de port de destination HTTPS 1000, les numéros de ports externes sont automatiquement calculés par rapport à ce numéro de port 1000 et utilisent respectivement 1001, 1002 et 1003.

Pour déployer un autre poste de travail virtuel, si le périphérique de mappage de ports a utilisé le numéro de port 1005 pour HTTPS, mappé à TCP 443, le numéro de port 1006 pour RDP, mappé à TCP 3389, le numéro de port 1007 pour PCoIP, mappé à TCP et UDP 4172, et le numéro de port 1008 pour le canal d'infrastructure, mappé à TCP 32111, avec exactement la même configuration de ports externes sur le poste de travail (+1, +2, +3, etc.), lorsque la connexion HTTPS provient d'un client qui a utilisé le numéro de port de destination HTTPS 1005, les numéros de port externes sont automatiquement calculés par rapport à ce numéro de port 1005 et utilisent respectivement les valeurs 1006, 1007 et 1008.

Ce schéma permet à tous les postes de travail d'être configurés de façon identique et de tous partager la même adresse IP externe. L'allocation des numéros de port par incréments de cinq (1000, 1005, 1010…) pour le numéro de port HTTPS de base permet donc de disposer de plus de 12 000 postes de travail virtuels accessible sur la même adresse IP. Le numéro de port de base sert à déterminer le poste de travail virtuel vers lequel acheminer la connexion, en fonction de la configuration du périphérique de mappage de ports. Pour une configuration `externalIPAddress`=10.20.30.40, `externalRDPPort=+1`, `externalPCoIPPort=+2` and `externalFrameworkChannelPort=+3` définie sur tous les postes de travail virtuels, le mappage à des postes de travail virtuels correspondrait à la description incluse dans la traduction d'adresses réseau et la table de mappage de ports.

Tableau 2-2. Valeurs de traduction d'adresses réseau et de mappage de ports

VM#	Adresse IP du poste de travail	HTTPS	RDP	PCOIP (TCP et UDP)	Canal d'infrastructure
0	192.168.0.0	10.20.30.40:1000 -> 192.168.0.0:443	10.20.30.40:1001 -> 192.168.0.0:3389	10.20.30.40:1002 -> 192.168.0.0:4172	10.20.30.40:1003 -> 192.168.0.0:32111
1	192.168.0.1	10.20.30.40:1005 -> 192.168.0.1:443	10.20.30.40:1006 -> 192.168.0.1:3389	10.20.30.40:1007 -> 192.168.0.1:4172	10.20.30.40:1008 -> 192.168.0.1:32111

Tableau 2-2. Valeurs de traduction d'adresses réseau et de mappage de ports (suite)

VM#	Adresse IP du poste de travail	HTTPS	RDP	PCOIP (TCP et UDP)	Canal d'infrastructure
2	192.168.0.2	10.20.30.40:1010 -> 192.168.0.2:443	10.20.30.40:1011 -> 192.168.0.2:3389	10.20.30.40:1012 -> 192.168.0.2:4172	10.20.30.40:1013 -> 192.168.0.2:32111
3	192.168.0.3	10.20.30.40:1015 -> 192.168.0.3:443	10.20.30.40:1016 -> 192.168.0.3:3389	10.20.30.40:1017 -> 192.168.0.3:4172	10.20.30.40:1018 -> 192.168.0.3:32111

Dans cet exemple, Horizon Client se connecte à l'adresse IP 10.20.30.40 et à un numéro de port de destination HTTPS (1000 + *n* * 5) où *n* est le numéro du poste de travail. Pour se connecter au poste de travail 3, le client se connecte à 10.20.30.40:1015. Ce schéma d'adressage simplifie de façon significative la configuration de chaque poste de travail. Tous les postes de travail sont configurés avec des configurations d'adresse externe et de port identiques. La configuration de la traduction d'adresses réseau et du mappage de ports est effectuée dans le périphérique de traduction d'adresses réseau et de mappage de port avec ce modèle cohérent, et tous les postes de travail sont accessibles sur une adresse IP publique unique. Le client utilise généralement un nom DNS public unique qui se résout à cette adresse IP.

Ajouter une autorité de certification à un magasin de certificats Windows

Pour l'authentification par carte à puce, l'autorité de certification (CA) qui signe les certificats de carte à puce doit exister dans le magasin de certificats Windows. . Sinon, vous pouvez ajouter l'autorité de certification au magasin de certificats Windows.

Conditions préalables

Vérifiez que Microsoft Management Console (MMC) dispose du composant logiciel enfichable Certificats. Reportez-vous à la section « Ajouter le composant logiciel enfichable Certificat à MMC » dans le document *Installation d'Horizon 7*.

Procédure

1. Démarrez MMC.
2. Dans la console MMC, développez le nœud **Certificats (Ordinateur local)** et allez dans le dossier **Autorités de certification racines de confiance > Certificats**.

   Si le certificat racine est présent et qu'il n'y a pas de certificats intermédiaires dans la chaîne de certificats, quittez MMC.
3. Cliquez avec le bouton droit sur le dossier **Autorités de certification racines de confiance > Certificats** et cliquez sur **Toutes les tâches > Importer**.
4. Dans l'assistant **Importation de certificat**, cliquez sur **Suivant** et allez à l'emplacement de stockage du certificat de l'autorité de certification racine.
5. Sélectionnez le fichier du certificat de l'autorité de certification racine et cliquez sur **Ouvrir**.

6 Cliquez sur **Suivant**, **Suivant** et **Terminer**.

7 Si le certificat de carte à puce est émis par une autorité de certification intermédiaire, importez tous les certificats intermédiaires de la chaîne de certificats.

   a Allez dans le dossier **Certificats (Ordinateur local) > Autorités de certification intermédiaires > Certificats**.

   b Recommencez les étapes 3 à 6 pour chaque certificat intermédiaire.

Configuration de HTML Access 3

Le plug-in View Agent Direct-Connection (VADC) prend en charge HTML Access vers des postes de travail basés sur une machine virtuelle et des postes de travail publiés. HTML Access vers des applications publiées n'est pas pris en charge.

Ce chapitre contient les rubriques suivantes :

Installer Horizon 7 Agent pour HTML Access

Pour prendre en charge HTML Access, vous devez installer Horizon 7 Agent sur le poste de travail basé sur une machine virtuelle avec un paramètre spécial.

Conditions préalables

- Téléchargez le fichier du programme d'installation d'Horizon Agent sur la page de téléchargement de VMware, à l'adresse http://www.vmware.com/go/downloadview.

  Le nom de fichier du programme d'installation est `VMware-Horizon-Agent-x86-y.y.y-xxxxxx.exe`, où *y.y.y* correspond au numéro de version et *xxxxxx* au numéro de build.

Procédure

- Installez Horizon 7 Agent à partir de la ligne de commande et spécifiez un paramètre qui indique à Horizon 7 Agent de ne pas s'enregistrer dans le Serveur de connexion Horizon 7.

  Cet exemple installe Horizon 7 Agent.

  ```
  VMware-Horizon-Agent-x86-y.y.y-xxxxxx.exe /v VDM_SKIP_BROKER_REGISTRATION=1
  ```

Étape suivante

Installez le plug-in View Agent Direct-Connection. Reportez-vous à la section Installer le plug-in View Agent Direct-Connection.

Configurer une livraison de contenu statique

Si le client HTML Access doit être desservi par le poste de travail, vous devez effectuer certaines tâches de configuration sur le poste de travail. Cela permet à un utilisateur de pointer un navigateur directement sur un poste de travail.

Conditions préalables

- Téléchargez le fichier zip `portal.war` d'Horizon HTML Access sur la page de téléchargement VMware, à l'adresse http://www.vmware.com/go/downloadview.

  Le nom de fichier est `VMware-Horizon-View-HTML-Access-`*`y.y.y`*`-`*`xxxxxx`*`.zip`, où *y.y.y* est le numéro de version et *xxxxxx* le numéro de build.

Procédure

1. Ouvrez **Panneau de configuration**.
2. Accédez à **Programmes et fonctionnalités > Activer ou désactiver des fonctionnalités Windows**.
3. Cochez la case **Services Internet (IIS)** et cliquez sur **OK**.
4. Dans **Panneau de configuration**, accédez à **Outils d'administration > Gestionnaires de services Internet Information (IIS)**.
5. Développez les éléments dans le volet de gauche.
6. Cliquez avec le bouton droit sur **Site Web par défaut**, puis sélectionnez **Modifier les liaisons...**.
7. Cliquez sur **Ajouter**.
8. Spécifiez **https**, **Toutes non attribuées**, et port **443**.
9. Dans le champ **Certificat SSL**, sélectionnez le certificat approprié.

Option	Action
Le certificat **vdm** est présent.	Sélectionnez **vdm** et cliquez sur **OK**.
Le certificat **vdm** n'est pas présent.	Sélectionnez **vdmdefault** et cliquez sur **OK**.

10. Dans la boîte de dialogue **Liaisons de sites**, supprimez l'entrée correspondant à **port http 80** et cliquez sur **Fermer**.
11. Cliquez sur **Site Web par défaut**.
12. Double-cliquez sur **Types MIME**.
13. Si **l'extension de nom de fichier** .json n'existe pas, dans le volet **Actions**, cliquez sur **Ajouter...**. Sinon, ignorez les 2 étapes suivantes.
14. Pour **Extension du nom de fichier**, entrez **.json**.
15. Pour **Type MIME**, entrez **text/h323** et cliquez sur **OK**.
16. Pour **Extension du nom de fichier**, entrez **.mem**.

17 Pour **Type MIME**, entrez **text/plain** et cliquez sur **OK**.

18 Copiez `VMware-Horizon-View-HTML-Access-y.y.y-xxxxxx.zip` dans un dossier temporaire.

19 Décompressez le fichier `VMware-Horizon-View-HTML-Access-y.y.y-xxxxxx.zip`.

Le résultat est un fichier nommé `portal.war`.

20 Renommez `portal.war` en `portal.zip`.

21 Décompressez le fichier `portal.zip` dans le dossier `C:\inetpub\wwwroot`.

Si nécessaire, modifiez les autorisations sur le dossier pour permettre l'ajout de fichiers.

Le dossier `C:\inetpub\wwwroot\portal` est créé.

22 Ouvrez **Bloc-notes**.

23 Créez le fichier `C:\inetpub\wwwroot\Default.htm` avec le contenu suivant (remplacez *<IP address or DNS name of desktop>* par l'adresse IP ou le nom DNS du poste de travail) :

```
<HEAD>
<noscript>
   <meta HTTP-EQUIV="REFRESH" content="0; url=https://<IP address or DNS name of desktop>/portal/
webclient/index.html">
</noscript>
</HEAD>
<script>
   var destination = 'https://<IP address or DNS name of desktop>/portal/webclient/index.html';
   var isSearch = !!window.location.search;
   window.location.href = destination + (isSearch ? window.location.search + '&' : '?') +
'vadc=1' + (window.location.hash || '');
</script>
```

Configurer un certificat de serveur TLS signé par une autorité de certification de confiance

Vous pouvez configurer un certificat du serveur TLS signé par une autorité de certification de confiance afin de garantir la sécurité du trafic entre les clients et les postes de travail.

Conditions préalables

- Remplacez le certificat de serveur TLS auto-signé par défaut par un certificat de serveur TLS signé par une autorité de certification de confiance. Reportez-vous à la section Remplacement du certificat de serveur TLS auto-signé par défaut. Cette opération crée un certificat portant le nom convivial **vdm**.
- Si le contenu statique du client est desservi par le poste de travail, configurez la livraison de contenu statique. Reportez-vous à la section Configurer une livraison de contenu statique.
- Familiarisez-vous avec le magasin de certificats de Windows. Reportez-vous à la section « Configurer le Serveur de connexion, le serveur de sécurité ou View Composer pour utiliser un nouveau certificat TLS » dans le document *Installation d'Horizon 7*.

Procédure

1. Dans le magasin de certificats de Windows, accédez à **Personnel > Certificats**.
2. Double-cliquez sur le certificat portant le nom convivial **vdm**.
3. Cliquez sur l'onglet **Détails**.
4. Copiez la valeur de **Empreinte numérique**.
5. Démarrez l'éditeur du Registre Windows.
6. Accédez à la clé de registre `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast \Config`.
7. Ajoutez une nouvelle valeur de chaîne (REG_SZ), `SSLHash`, à cette clé de registre.
8. Définissez la valeur `SSLHash` sur la valeur **Empreinte numérique**.

Désactiver le protocle HTTP/2 sur des postes de travail Windows 10 et Windows 2016

Avec certains navigateurs Web, vous pouvez rencontrer l'erreur ERR_SPDY_PROTOCOL_ERROR lorsque vous accédez à un poste de travail Windows 10 VADC ou Windows 2016 VADC. Vous pouvez éviter cette erreur en désactivant le protocole HTTP/2 sur le poste de travail.

Procédure

1. Démarrez l'éditeur du Registre Windows.
2. Accédez à la clé de registre `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\HTTP \Parameters`.
3. Ajoutez 2 nouvelles valeurs REG_DWORD, `EnableHttp2Tls` et `EnableHttp2Cleartext`, à cette clé de registre.
4. Réglez les deux valeurs sur **0**.
5. Redémarrez le poste de travail.

Configuration de View Agent Direct Connection sur des hôtes des services Bureau à distance (RDS)

4

Horizon 7 prend en charge les hôtes des services Bureau à distance (RDS) qui fournissent des applications et des postes de travail publiés auxquels les utilisateurs ont accès à partir d'instances d'Horizon Client. Un poste de travail publié est basé sur une session de poste de travail ouverte sur un hôte RDS. Dans un déploiement Horizon 7 classique, les clients se connectent à des postes de travail et à des applications via le Serveur de connexion Horizon. Cependant, si vous installez le plug-in View Agent Direct-Connection sur un hôte RDS, les clients peuvent se connecter directement à des applications ou des postes de travail publiés sans utiliser le Serveur de connexion Horizon.

Ce chapitre contient les rubriques suivantes :

Hôtes des services Bureau à distance

Un hôte des services Bureau à distance (RDS) est un ordinateur serveur qui héberge des applications et des postes de travail pour un accès distant.

Dans un déploiement Horizon 7, un hôte RDS est un serveur Windows qui dispose du rôle Services Bureau à distance Microsoft, du service Hôte de session Bureau à distance Microsoft, et sur lequel Horizon Agent est installé. Un hôte RDS peut prendre en charge View Agent Direct Connection (VADC) si le plug-in VADC y est également installé. Pour plus d'informations sur la configuration d'un hôte RDS et sur l'installation d'Horizon 7 Agent, reportez-vous à la section « Configuration d'hôtes de services Bureau à distance » dans le document *Configuration d'applications et de postes de travail publiés dans Horizon 7*. Pour plus d'informations sur l'installation du plug-in VADC, reportez-vous à Chapitre 1 Installation du plug-in View Agent Direct-Connection.

Note Lorsque vous installez Horizon Agent, le programme d'installation demande le nom d'hôte ou l'adresse IP du Serveur de connexion Horizon auquel Horizon Agent se connectera. Vous pouvez exécuter le programme d'installation avec un paramètre lui demandant d'ignorer cette étape.

```
VMware-Horizon-Agent-x86-y.y.y-xxxxxx.exe /v "VDM_SKIP_BROKER_REGISTRATION=1"
```

Après avoir configuré un hôte RDS et installé le plug-in VADC, vous devez octroyer des postes de travail et des applications RDS. Reportez-vous à la section Autoriser des applications et des postes de travail publiés.

Autoriser des applications et des postes de travail publiés

Vous devez autoriser les utilisateurs afin qu'ils puissent accéder aux applications et aux postes de travail publiés.

Si l'hôte RDS exécute Windows Server 2008 R2 SP1, exécutez le **Gestionnaire RemoteApp** pour configurer les droits d'accès.

Si l'hôte RDS exécute Windows Server 2012 ou 2012 R2, exécutez le **Gestionnaire de serveur** et accédez à **Services Bureau à distance** pour configurer les droits d'accès.

Autorisations de poste de travail

Pour autoriser un utilisateur à lancer un poste de travail publié, exécutez les étapes suivantes :

- Vérifiez que l'utilisateur est membre du groupe local **Utilisateurs de View Agent Direct-Connection**. Par défaut, tous les utilisateurs authentifiés sont membres de ce groupe.
- Pour Windows Server 2008 R2 SP1, dans **Gestionnaire RemoteApp**, vérifiez que le serveur Hôte de session Bureau à distance est configuré sur **Afficher une connexion Bureau à distance sur ce serveur hôte de session Bureau à distance dans l'accès Bureau à distance par le Web**.
- Pour Windows 2012 ou 2012 R2, exécutez le **Gestionnaire de serveur** et accédez à **Services Bureau à distance** pour configurer les droits d'accès. Utilisez l'assistant de démarrage rapide pour déployer les services RDSH.

Autorisations d'application

Pour autoriser un utilisateur à lancer une application, exécutez les étapes suivantes :

- Vérifiez que l'utilisateur est membre du groupe local **Utilisateurs de View Agent Direct-Connection**. Par défaut, tous les utilisateurs authentifiés sont membres de ce groupe.
- Pour Windows Server 2008 R2 SP1, dans le **Gestionnaire RemoteApp**, vérifiez que l'application est répertoriée sous **Programmes RemoteApp**, qu'elle est définie pour l'**Accès Bureau à distance par le Web** et qu'elle dispose d'attributions d'utilisateurs définies pour tous les utilisateurs, pour cet utilisateur ou pour un groupe dont l'utilisateur est membre.
- Pour Windows 2012 ou 2012 R2, exécutez le **Gestionnaire de serveur** et accédez à **Services Bureau à distance** pour configurer les droits d'accès.

Dépannage du plug-in View Agent Direct-Connection 5

Lorsque vous utilisez le plug-in View Agent Direct-Connection, vous pouvez rencontrer des problèmes connus.

Lorsque vous enquêtez sur un problème lié au plug-in View Agent Direct-Connection, vérifiez que la version correcte est installée et en cours d'exécution.

Si vous devez poser une question à VMware concernant le support technique, activez toujours la journalisation complète, reproduisez le problème et générez un jeu de journaux DCT (Data Collection Tool). Le support technique de VMware peut ensuite analyser ces journaux. Pour plus d'informations sur la génération d'un jeu de journaux DCT, reportez-vous à l'article de la base de connaissances de VMware sur la collecte d'informations de diagnostic http://kb.vmware.com/kb/1017939.

Ce chapitre contient les rubriques suivantes :

Le pilote graphique installé est incorrect

Pour que PCoIP fonctionne correctement, la version appropriée du pilote graphique doit être installée.

Problème

Un écran noir apparaît lorsqu'un utilisateur se connecte à un poste de travail ou à une application à l'aide du protocole PCoIP.

Cause

Une version incorrecte du pilote graphique est en cours d'exécution. Cela se produit si une version incorrecte de VMware Tools est installée après l'installation de Horizon 7 Agent.

Solution

- Réinstallez Horizon 7 Agent.

RAM vidéo insuffisante

Pour prendre en charge le protocole PCoIP, une machine virtuelle qui exécute un poste de travail ou un hôte RDS doit disposer d'au moins 128 Mo de RAM vidéo.

Problème

Un écran noir apparaît lorsqu'un utilisateur se connecte à un poste de travail ou à une application à l'aide du protocole PCoIP.

Cause

La machine virtuelle ne dispose pas de suffisamment de RAM vidéo.

Solution

- Configurez au moins 128 Mo de RAM vidéo pour chaque machine virtuelle.

Activation de la journalisation complète pour inclure les informations de suivi et de débogage

Le plug-in View Agent Direct-Connection écrit des entrées de journal dans le journal standard d'Horizon Agent. Par défaut, les informations TRACE et DEBUG ne sont pas incluses dans le journal.

Problème

Le journal de Horizon 7 Agent ne contient pas d'informations TRACE et DEBUG.

Cause

La journalisation complète n'est pas activée. Vous devez activer la journalisation complète pour inclure les informations TRACE et DEBUG dans le journal d'Horizon Agent.

Solution

1. Ouvrez une fenêtre d'invite de commande et exécutez `C:\Program Files\VMware\VMware View\Agent\DCT\support.bat loglevels`
2. Entrez **3** pour une journalisation complète.

   Les fichiers journaux de débogage se trouvent dans `%ALLUSERSPROFILE%\VMware\VDM\logs`. Le fichier `debug*.log` contient les informations consignées depuis Horizon Agent et le plug-in. Recherchez `wsnm_xmlapi` pour trouver les lignes de journal du plug-in.

   Lorsqu'Horizon Agent démarre, la version du plug-in est consignée :

   ```
   2012-10-01T12:09:59.078+01:00 INFO (09E4-0C08) <logloaded> [MessageFrameWork] Plugin 'wsnm_xmlapi - VMware View Agent XML API Handler Plugin' loaded, version=e.x.p build-855808, buildtype=release
   ```

   ```
   2012-10-01T12:09:59.078+01:00 TRACE (09E4-06E4) <PluginInitThread> [wsnm_xmlapi] Agent XML API Protocol Handler starting
   ```