Administration du plug-in VMware Horizon View Agent Direct-Connection

Horizon View 5.3
View Agent 5.3

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

FR-001290-00

vmware®

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

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

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

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

docfeedback@vmware.com

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

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

Table des matières

Administration du plug-in VMware Horizon View Agent Direct-Connection

Administration du plug-in VMware Horizon View Agent Direct-Connection fournit des informations sur l'installation et la configuration du plug-in Horizon View Agent Direct-Connection. Ce plug-in est une extension installable de View Agent qui permet à View Client de se connecter directement à un poste de travail View sans utiliser le Serveur de connexion View.

Avec le plug-in VMware Horizon View Agent Direct-Connection qui s'exécute sur un poste de travail virtuel, le client peut se connecter directement au poste de travail virtuel. Toutes les fonctionnalités du poste de travail View concernant PCoIP, HTML5 Access, RDP, la redirection USB et la gestion de sessions fonctionnent de la même manière que lorsque l'utilisateur se connecte via le Serveur de connexion View.

Public visé

Ces informations sont destinées à toute personne qui souhaite installer, mettre à jour ou utiliser le plug-in VMware Horizon View Agent Direct-Connection sur le poste de travail virtuel VMware. Le manuel s'adresse à des administrateurs expérimentés du système Windows qui connaissent bien la technologie des machines virtuelles et le fonctionnement des datacenters.

Installation et configuration du plug-in VMware Horizon View Agent Direct-Connection

1

Lorsque vous installez le plug-in Horizon View Agent Direct-Connection, vérifiez d'abord que le poste de travail View possède certains éléments de configuration système requis, puis exécutez le programme d'installation sur la machine virtuelle.

Ce chapitre aborde les rubriques suivantes :

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

Le plug-in Horizon View Agent Le plug-in Direct-Connection doit être installé sur un poste de travail virtuel View possédant certains éléments de configuration logicielle spécifiques.

Tableau 1-1. Configuration système requise pour le plug-in Horizon View Agent Direct-Connection

Versions de vSphere	Versions du système d'exploitation	Logiciel
Toutes les versions vSphere prises en charge par la version de View Agent spécifiée. IMPORTANT Tous les postes de travail virtuels doivent être hébergés sur des hôtes vSphere 5.x ESXi.	Toutes les versions du système d'exploitation prises en charge par la version de View Agent spécifiée.	■ View Agent 5.3 ou version ultérieure ■ Vous devez installer Horizon View Agent après avoir installé VMware Tools.

IMPORTANT Chaque poste de travail virtuel View doit être configuré avec un minimum de 128 Mo de RAM vidéo pour que le protocole PCoIP fonctionne correctement.

Le poste de travail virtuel peut être associé à un domaine Microsoft Active Directory ou appartenir à un groupe de travail.

Installation du plug-in VMware Horizon View Agent Direct-Connection

Vous devez installer le plug-in Horizon View Agent Direct-Connection sur une machine virtuelle Windows qui exécute View Agent.

Prérequis

Vérifiez que la machine virtuelle exécute une version prise en charge de View Agent, qu'elle dispose de suffisamment de RAM vidéo et qu'elle s'exécute sur une version prise en charge de ESXi. Reportez-vous à la section « Configuration système requise pour le plug-in VMware Horizon View Agent Direct-Connection », page 7.

Procédure

1 Connectez-vous à la machine virtuelle en tant qu'administrateur et lancez le programme d'installation correspondant à votre système d'exploitation.

Système d'exploitation	Programme d'installation
Windows 64 bits	`VMware-viewagent-direct-connection-x86_64-x.y.z-nnnnnn.exe`
Windows 32 bits	`VMware-viewagent-direct-connection-x.y.z-nnnnnn.exe`

Le programme d'installation vérifie que les versions correctes du système d'exploitation Windows et de View Agent sont installées.

2 Éventuellement, dans la boîte de dialogue Informations de configuration, saisissez le numéro de port TCP utilisé par le plug-in pour écouter les requêtes HTTPS entrantes provenant des clients View Client.

Le numéro de port TCP par défaut est 443 et ne doit pas être modifié dans la plupart des cas ; toutefois, en cas de besoin, vous pouvez le modifier après l'installation.

La case à cocher **[Configurer automatiquement le pare-feu Windows]** est sélectionnée par défaut. Cette sélection ajoute une règle de pare-feu pour que ce port TCP accepte les connexions provenant des clients View. Si le pare-feu Windows s'exécute et si cette règle n'a pas été créée, les clients View Client ne pourront pas se connecter.

Suivant

Une fois l'installation terminée, testez-la en utilisant View Client pour accéder à cette machine virtuelle. Dans View Client, au lieu d'indiquer le nom ou l'adresse IP d'une instance du Serveur de connexion View ou du serveur de sécurité, spécifiez le nom ou l'adresse IP d'un poste de travail View qui exécute ce plug-in. L'authentification se fait selon la procédure habituelle et les processus de sélection du poste de travail et de connexion à celui-ci sont les mêmes que lors d'une connexion via le Serveur de connexion View.

Désinstallation du plug-in VMware Horizon View Agent Direct-Connection

Vous pouvez désinstaller le plug-in Horizon View Agent Direct-Connection comme n'importe quelle autre application Windows.

Procédure

1 Accédez au **[Panneau de configuration > Programmes et fonctionnalités.]**

2 Sélectionnez **[VMware View Agent Direct-Connection Plugin.]**

3 Sélectionnez **[Désinstaller.]**

Le plug-in Horizon View Agent Direct-Connection est supprimé et View Agent redémarre.

Configuration avancée du plug-in VMware Horizon View Agent Direct-Connection

2

Vous pouvez utiliser les paramètres de configuration par défaut du plug-in Horizon View Direct-Connection ou les personnaliser à l'aide des stratégies de groupe (GPO) de Windows Active Directory ou de certains paramètres du registre Windows.

Ce chapitre aborde les rubriques suivantes :

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

Tous les paramètres de configuration pour le plug-in Horizon View Agent Direct-Connection sont stockés dans le registre local sur chaque poste de travail View. Vous pouvez contrôler ces paramètres en utilisant les stratégies de groupe (GPO) de Windows Active Directory, l'éditeur de stratégie local ou en modifiant directement le registre.

Le plug-in utilise des valeurs par défaut. Toutefois, vous pouvez les modifier. Les valeurs du registre peuvent être définies dans la clé de registre :

```
HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Agent\Configuration\XMLAPI
```

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

Paramètre	Valeur du registre	Type	Description
Numéro de port HTTPS	httpsPortNumber	REG_SZ	Numéro de port TCP sur lequel le plug-in écoute les requêtes HTTPS entrantes envoyées par View Client. Si vous modifiez cette valeur, vous devez effectuer la modification correspondante dans le pare-feu Windows afin que la nouvelle valeur soit acceptée.
Délai d'expiration de la session	sessionTimeout	REG_SZ	Période pendant laquelle un utilisateur peut garder une session ouverte après s'être connecté avec View Client. La valeur est définie en minutes. Si cette stratégie n'est pas configurée ou si elle est désactivée, la valeur par défaut est de 600 minutes. Lorsque le délai d'une session de poste de travail expire, la session prend fin et View Client est déconnecté du poste de travail.

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

Paramètre	Valeur du registre	Type	Description
Exclusion de responsabilité activée	disclaimerEnabled	REG_SZ	La valeur est définie à `TRUE` ou `FALSE`. Si elle est égale à `TRUE`, le texte d'exclusion de responsabilité que l'utilisateur doit accepter au moment de la connexion s'affiche. Il correspond au « Texte d'exclusion de responsabilité » si celui-ci a été rédigé, ou il est extrait de la GPO `Configuration\Windows Settings\Security Settings\Local Policies\Security Options: Interactive logon`. Par défaut, disclaimerEnabled est défini à `FALSE`.
Texte d'exclusion de responsabilité	disclaimerText	REG_SZ	Texte d'exclusion de responsabilité que voient les utilisateurs de View Client au moment de la connexion. La stratégie Exclusion de responsabilité activée doit être définie à `TRUE`. Si le texte n'est pas spécifié, la valeur par défaut utilisée est celle de la stratégie Windows `Configuration\Windows Settings\Security Settings\Local Policies\Security Options`.
Paramètre Client : AlwaysConnect	alwaysConnect	REG_SZ	La valeur est définie à `TRUE` ou `FALSE`. Le paramètre AlwaysConnect est envoyé à View Client. Si cette stratégie est définie à `TRUE`, elle remplace les préférences client enregistrées. Aucune valeur n'est définie par défaut. L'activation de cette stratégie définit la valeur à `TRUE`. La désactivation de cette stratégie définit la valeur à `FALSE`.
Port PCoIP externe	externalPCoIPPort	REG_SZ	Numéro de port envoyé à View Client pour le numéro de port TCP/UDP de destination utilisé avec le protocole PCoIP. Le signe + devant le numéro indique que celui-ci est calculé par rapport au numéro de port utilisé avec HTTPS. Ne définissez cette valeur que si le numéro de port exposé à l'extérieur 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 Blast externe	externalBlastPort	REG_SZ	Numéro de port envoyé à View Client pour le numéro de port TCP de destination utilisé avec le protocole HTML5/Blast. Le signe + devant le numéro indique que celui-ci est calculé par rapport au numéro de port utilisé avec HTTPS. Ne définissez cette valeur que si le numéro de port exposé à l'extérieur 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	externalRDPPort	REG_SZ	Numéro de port envoyé à View Client pour le numéro de port TCP de destination utilisé avec le protocole RDP. Le signe + devant le numéro indique que celui-ci est calculé par rapport au numéro de port utilisé avec HTTPS. Ne définissez cette valeur que si le numéro de port exposé à l'extérieur 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.

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

Paramètre	Valeur du registre	Type	Description
Adresse IP externe	externalIPAddress	REG_SZ	Adresse IP v4 envoyée à View 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 à l'extérieur ne correspond pas à celle du poste de travail. En général, cette adresse s'utilise dans un environnement NAT. Aucune valeur n'est définie par défaut.
Port Framework Channel externe	externalFrameworkChannelPort	REG_SZ	Numéro de port envoyé à View Client pour le numéro de port TCP de destination utilisé avec le protocole Framework Channel. Le signe + devant le numéro indique que celui-ci est calculé par rapport au numéro de port utilisé avec HTTPS. Ne définissez cette valeur que si le numéro de port exposé à l'extérieur 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.
USB activé	usbEnabled	REG_SZ	La valeur est définie à `TRUE` ou `FALSE`. Détermine si les postes de travail peuvent utiliser des périphériques USB connectés au système client. Par défaut, ce paramètre est activé. Pour empêcher l'utilisation de périphériques externes pour des raisons de sécurité, désactivez le paramètre (valeur `FALSE`).
Paramètre Client : Connexion USB automatique	usbAutoConnect	REG_SZ	La valeur est définie à `TRUE` ou `FALSE`. Les périphériques USB sont connectés au poste de travail lors de leur insertion. Si cette stratégie est définie, elle remplace les préférences client sauvegardées. Aucune valeur n'est définie par défaut.
Réinitialisation activée	resetEnabled	REG_SZ	La valeur est définie à `TRUE` ou `FALSE`. Si elle est égale à `TRUE`, un client View Client authentifié peut effectuer un redémarrage au niveau du système d'exploitation. Le paramètre par défaut est désactivé (`FALSE`).
Délai de mise en cache des informations d'identification du client	clientCredentialCacheTimeout	REG_SZ	Délai, exprimé en minutes, pendant lequel View Client autorise un utilisateur à se servir d'un mot de passe sauvegardé. 0 correspond à Jamais, -1 correspond à Toujours. View Client permet aux utilisateurs de sauvegarder leurs mots de passe lorsque ce paramètre est défini sur une valeur valide. La valeur par défaut est 0 (jamais).

Les paramètres de View Client ne modifient pas le comportement du plug-in. Ils sont transmis à View Client pour interprétation.

Les numéros de ports externes et les valeurs des adresses IP externes sont utilisées pour prendre en charge la traduction d'adresses réseau (NAT, Network Address Translation) et le mappage des ports. Pour plus d'informations, reportez-vous à « Utilisation du système NAT et du mappage de ports », page 13.

Vous pouvez définir des stratégies qui remplacent ces paramètres du registre à l'aide de l'Éditeur de stratégie local ou des objets de stratégie de groupe (GPO, Group Policy Object) d'Active Directory. Les paramètres de stratégie sont prioritaires par rapport aux paramètres normaux du registre. Un fichier modèle GPO est fourni pour configurer les stratégies. Lorsque View Agent et le plug-in sont installés dans l'emplacement par défaut, le fichier modèle se trouve dans :

```
C:\Program Files\VMware\VMware View\Agent\extras\view_agent_direct_connection.adm
```

Vous pouvez importer ce fichier modèle dans Active Directory ou dans l'Éditeur de stratégie de groupe local pour simplifier la gestion des paramètres de configuration. Pour plus d'informations sur la gestion des paramètres de stratégie de cette manière, reportez-vous à la documentation relative à l'Éditeur de stratégie Microsoft et à la gestion des GPO. Les paramètres de stratégie pour le plug-in sont stockés dans la clé de registre :

`HKEY_LOCAL_MACHINE Software\Policies\VMware, Inc.\VMware VDM\Agent\Configuration\XMLAPI`

Désactivation des chiffrements faibles dans SSL/TLS

Cette procédure vous permet de veiller à ce que les communications entre View Client et le poste de travail View transitant par le protocole SSL/TLS n'acceptent pas les algorithmes de chiffrement faible.

Les paramètres pour désactiver les chiffrements faibles sont stockés dans le registre Windows. La modification de ces paramètres doit être effectuée sur le système d'exploitation de tous les postes de travail qui exécutent le plug-in View Agent Direct-Connection.

Remarque Ces paramètres affectent tous les aspects de l'utilisation du protocole SSL/TLS sur le système d'exploitation.

SSL 3.0 et TLS 1.0 (RFC2246) avec INTERNET-DRAFT `56-bit Export Cipher Suites For TLS draft-ietf-tls-56-bit-ciphersuites-00.txt` proposent des options permettant d'utiliser différentes suites de chiffrement. Chaque suite détermine l'échange de clés, l'authentification, le cryptage et les algorithmes MAC utilisés pendant une session SSL/TLS.

Prérequis

Vous devez avoir une expérience de la modification des clés de registre Windows à l'aide l'éditeur de registre `Regedt32.exe`.

Procédure

- Démarrez l'Éditeur de registre `Regedt32.exe` et recherchez la clé :`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL`

Suivant

Tableau 2-2. Mises à jour des suites de chiffrement

Windows XP SP3	Windows Vista et versions ultérieures
1 Dans la sous-clé `\Ciphers\DES 56/56`, ajoutez une valeur DWORD `Enabled` avec une valeur de `0x0`. 2 Dans la sous-clé `\Hashes\MD5`, ajoutez une valeur DWORD `Enabled` avec une valeur de `0x0`. Ces mises à jour garantissent que seuls les chiffrements suivants sont disponibles dans Windows XP SP3 : ■ SSLv3 168 bits DES-CBC3-SHA ■ SSLv3 128 bits RC4-SHA ■ TLSv1 168 bits DES-CBC3-SHA ■ TLSv1 128 bits RC4-SHA	1 Dans la sous-clé `\Hashes`, créez une sous-clé `MD5`. 2 Dans la sous-clé `\Hashes \MD5`, ajoutez une valeur DWORD `Enabled` avec une valeur de `0x0`. Ces mises à jour garantissent que seuls les chiffrements suivants sont disponibles dans Windows Vista et les versions ultérieures : ■ SSLv3 168 bits DES-CBC3-SHA ■ SSLv3 128 bits RC4-SHA ■ TLSv1 256 bits AES256-SHA ■ TLSv1 128 bits AES128-SHA ■ TLSv1 168 bits DES-CBC3-SHA ■ TLSv1 128 bits RC4-SHA

Remplacement du certificat serveur SSL auto-signé par défaut

Un certificat serveur SSL auto-signé n'offre pas à View Client une protection suffisante contre la fraude et l'espionnage. 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 serveur SSL auto-signé qu'il place dans le magasin de certificats Windows. Le certificat serveur SSL est présenté à View Client durant la phase de négociation du protocole SSL afin de lui transmettre des informations sur le poste de travail View. Ce certificat SSL auto-signé par défaut ne peut pas apporter de garantie sur ce poste de travail tant qu'il n'est pas remplacé par un certificat signé par une Autorité de certification (CA) approuvée par le client et que View Client ne l'a pas entièrement validé en effectuant des vérifications de certificat.

La procédure pour stocker ce certificat dans le Magasin de certificats Windows et le remplacer par un certificat signé approprié émis par une autorité de certification sont les mêmes que celles utilisées pour le Serveur de connexion View (version 5.1 ou ultérieure). Voir « Configuration de certificats SSL pour les serveurs View » dans le document d'installation de VMware Horizon View pour plus de détails sur le remplacement du certificat.

Les certificats avec un Autre nom de sujet (SAN) et les certificats avec caractères génériques sont pris en charge.

Remarque Pour diffuser les certificats de serveur SSL signés par une CA à un grand nombre de postes de travail View exécutant le plug-in View Agent Direct-Connection, utilisez l'inscription à Active Directory pour distribuer les certificats sur chaque machine virtuelle. Pour plus d'informations, reportez-vous à : http://technet.microsoft.com/en-us/library/cc732625.aspx

---

Autoriser View Client à accéder au poste de travail View

Le mécanisme d'autorisation qui permet à un utilisateur de View Client d'accèder directement au poste de travail View est contrôlé par un groupe local du système d'exploitation appelé **[Utilisateurs de View Agent Direct-Connection]** .

Si un utilisateur est membre de ce groupe, il est autorisé à se connecter directement au poste de travail. Ce groupe local est créé au moment d'installation initiale du plug-in et contient le groupe Utilisateurs authentifiés. Quiconque est authentifié par le plug-in peut accéder au poste de travail.

Pour restreindre l'accès au poste de travail, vous pouvez modifier l'appartenance à ce groupe de façon à établir une liste d'utilisateurs et de groupes d'utilisateurs. Il peut s'agir d'utilisateurs locaux ou de domaines et de groupes d'utilisateurs. Si l'utilisateur de View Client n'appartient pas à ce groupe, il reçoit un message après authentification lui indiquant qu'il n'a pas accès au poste de travail.

Utilisation du système NAT et du mappage de ports

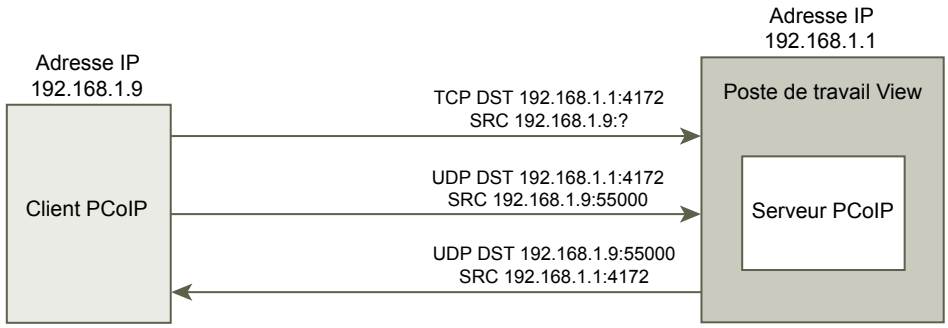
Le système NAT (Network Address Translation) et la fonction de mappage de ports sont nécessaires si les clients View Client se connectent à des postes de travail View sur des réseaux différents.

Dans les exemples fournis, vous devez configurer des informations d'adressage externe sur le poste de travail View afin que View Client puisse les utiliser pour se connecter au poste de travail View à l'aide du système NAT ou d'un périphérique de mappage de ports. Cette URL est la même que celle établie dans les paramètres URL externe et URL externe PCoIP définis sur le Serveur de connexion View et sur le serveur de sécurité.

Lorsque View Client est situé sur un réseau différent et qu'un périphérique NAT se trouve entre View Client et le poste de travail virtuel View exécutant le plug-in, une configuration NAT ou de mappage de ports est nécessaire. Par exemple, s'il existe un pare-feu entre View Client et le poste de travail virtuel View, ce pare-feu agit comme un système NAT ou un périphérique de mappage de ports.

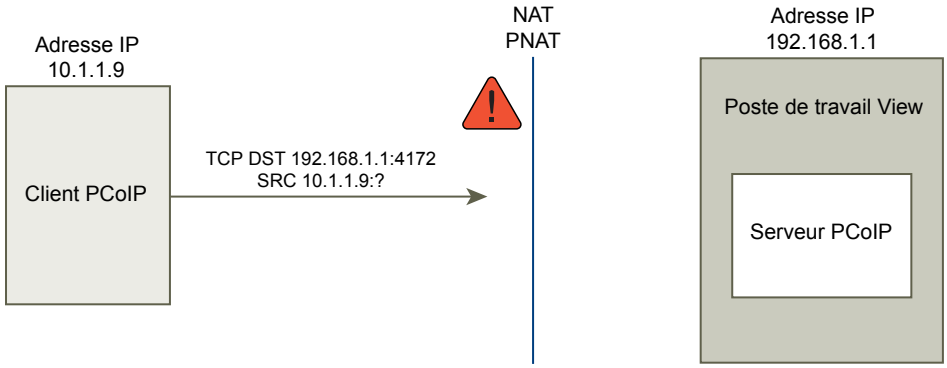
L'exemple de déploiement d'un poste de travail View dont l'adresse IP est 192.168.1.1 illustre la configuration d'un système NAT et du mappage de ports. Un système View Client dont l'adresse IP est 192.168.1.9 sur le même réseau établit une connexion PCoIP en utilisant TCP et UDP. Cette connexion se fait directement, sans configuration de système NAT ou de mappage de ports.

Figure 2-1. Connexion PCoIP directe d'un client sur le même réseau



Si vous ajoutez un périphérique NAT entre le client et le poste de travail de façon que les deux systèmes fonctionnent dans un espace d'adressage différent et que vous ne modifiiez pas la configuration du plug-in, les paquets PCoIP ne seront pas acheminés correctement et leur transmission échouera. Dans cet exemple, le client utilise un espace d'adressage différent et son adresse IP est 10.1.1.9. Cette configuration n'est pas correcte, car le client va utiliser 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 depuis le réseau client et peut entraîner l'affichage d'un écran noir sur le client.

Figure 2-2. Échec de la connexion PCoIP depuis un client via un périphérique NAT

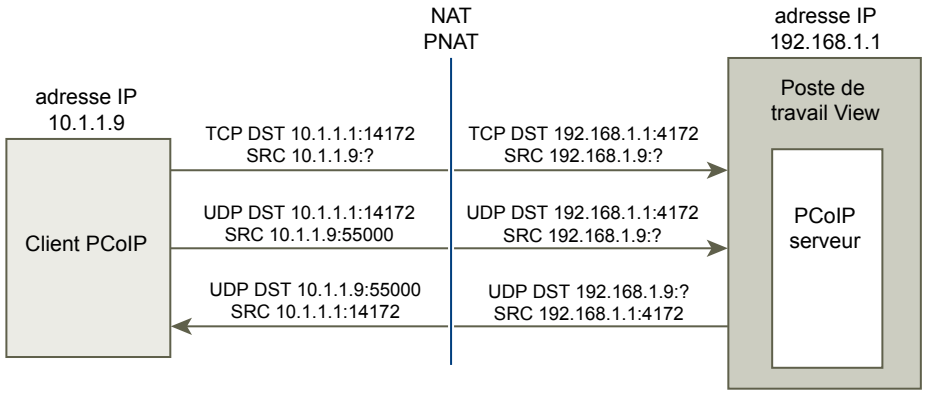


Pour résoudre le problème, vous devez configurer le plug-in de telle sorte qu'il utilise une adresse IP externe. Si `externalIPAddress` est configuré avec la valeur 10.1.1.1 pour ce poste de travail, le plug-in fournit au client l'adresse IP 10.1.1.1 lors de l'établissement de connexions au poste de travail via le protocole de poste de travail. Pour PCoIP, avec cette configuration, le service PCoIP Secure Gateway doit être démarré sur le poste de travail.

En matière de mappage de ports, lorsque le poste de travail utilise le port standard PCoIP 4172 et que le client doit utiliser un port de destination différent mappé sur le port 4172 sur le périphérique de mappage de ports, vous devez configurer le plug-in en conséquence. Si le périphérique de mappage de ports mappe le port 14172 sur 4172, le client doit utiliser 14172 comme port de destination pour PCoIP. Vous devez définir cette configuration pour le protocole PCoIP. Définissez `externalPCoIPPort`dans le plug-in sur 14172.

Dans une configuration utilisant le système NAT et le mappage de ports, `externalIPAdress` est défini sur 10.1.1.1, traduit 192.168.1.1 par NAT, et `externalPColPPort` est défini sur 14142, qui est mappé sur le port 4172.

Figure 2-3. Connexion PCoIP depuis un client via un périphérique NAT et le mappage de ports



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

Schéma d'adressage avancé

Lorsque vous configurez plusieurs postes de travail View afin qu'ils soient accessibles via un système NAT et un périphérique de mappage de ports sur la même adresse IP externe, vous devez attribuer à chaque poste un ensemble unique de numéros de port. Les clients peuvent ensuite employer la même adresse IP de destination, mais ils utilisent un numéro de port TCP unique pour la connexion HTTPS afin de la diriger vers un poste de travail virtuel spécifique.

Exemples de schéma d'adressage

Dans cet exemple, le port HTTPS 1000 renvoie vers un poste de travail et le port HTTPS 1005 renvoie vers un autre poste ; dans les deux cas, la même adresse IP de destination est utilisée. Dans ce cas, il serait trop complexe de configurer des numéros de ports externes uniques pour chaque poste de travail View pour permettre les connexions via le protocole du poste de travail. C'est pourquoi les paramètres de plug-in `externalPCoIPPort`, `externalRDPPort` et `externalFrameworkChannelPort` acceptent une expression relationnelle facultative à la place d'une valeur statique pour définir un numéro de port par rapport au numéro de port HTTPS de base utilisé par le client.

Si le périphérique de mappage de ports utilise pour HTTPS le numéro de port 1000 mappé sur TCP 443, le port 1001 pour RDP mappé sur TCP 3389, le port 1002 pour PCoIP mappé sur le port 4172 TCP et UDP et le port 1003 pour Framework Channel mappé sur TCP 32111, il est possible, dans un souci de simplification, de configurer les numéros de ports externes selon le schéma suivant : `externalRDPPort=+1`, `externalPCoIPPort=+2` et `externalFrameworkChannelPort=+3`. Lorsque la connexion HTTPS est établie depuis un client qui utilise le port de destination HTTPS 1000, les numéros de ports externes sont automatiquement calculés par rapport à ce numéro 1000 et prennent respectivement les valeurs 1001, 1002 et 1003.

En cas de déploiement d'un autre poste de travail virtuel, si le périphérique de mappage utilise le numéro 1005 pour HTTPS mappé sur TCP 443, le port 1006 pour RDP mappé sur TCP 3389, le port 1007 pour PCoIP mappé sur TCP et UDP 4172 et le port 1008 pour le Framework Channel mappé sur TCP 32111, avec la même configuration de ports externes sur le poste de travail (+1, +2, +3, etc.), lorsque la connexion HTTPS est établie depuis un client utilisant le port de destination HTTPS 1005, les numéros de ports externes sont automatiquement calculés par rapport à ce numéro 1005 et prennent respectivement les valeurs 1006, 1007 et 1008.

Ce schéma permet à tous les postes de travail View d'être configurés de manière identique tout en partageant la même adresse IP externe. L'allocation de numéros de ports par incrément de cinq (1000, 1005, 1010 …) pour le numéro port HTTPS de base permet par conséquent d'accéder à plus de 12 000 postes de travail virtuels sur la même adresse IP et, avec le numéro de port de base, de déterminer le poste de travail virtuel vers lequel diriger la connexion, selon la configuration du périphérique de mappage de port. Si tous les postes de travail virtuels sont configurés avec les valeurs `externalIPAddress`=10.20.30.40, `externalRDPPort`=+1, `externalPCoIPPort`=+2 et `externalFrameworkChannelPort`=+3, le mappage vers des postes de travail virtuels correspond à ce qui est indiqué dans le tableau Système NAT et mappage des ports.

Tableau 2-3. Système NAT et valeurs de mappage des ports

VM#	Adresse IP du poste de travail	HTTPS	RDP	PCOIP (TCP et UDP)	Framework Channel
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
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

View Client se connecte à l'adresse IP 10.20.30.40 et à un port de destination HTTPS dont la valeur est (1000 + *n* * 5) où *n* est le numéro du poste de travail View. Pour se connecter au poste de travail View 3, le client se connectera à l'adresse 10.20.30.40:1015. Ce schéma d'adressage simplifie considérablement la configuration de chaque poste de travail View. Tous les postes de travail sont configurés avec des paramètres de port et d'adresse externe identiques. La configuration NAT et de mappage des ports est effectuée dans le périphérique NAT et de mappage selon ce schéma cohérent et tous les postes de travail View sont accessibles sur une adresse IP publique unique. Le client utilise habituellement un nom de DNS public unique dont la résolution renvoie à cette adresse IP.

Dépannage du plug-in VMware Horizon View Agent Direct-Connection

3

Lors de l'utilisation du plug-in Horizon View Agent Direct-Connection, il peut arriver que vous rencontriez des problèmes connus et soyez amené à les résoudre.

Lorsque vous examinez un problème survenu dans le plug-in Horizon View Agent Direct-Connection, assurez-vous que la version installée qui s'exécute est la bonne. Dans l'exemple ci-dessus, les informations de version du plug-in sont `version=e.x.p build-855808, buildtype=release`. Le nom du plug-in, VMware View Agent XML API Handler Plugin, est consigné dans le fichier journal.

Si un problème doit être soumis au Support technique de VMware, activez toujours la journalisation complète, reproduisez le problème et générez un groupe de journaux DCT (Data Collection Tool). Le Support technique analysera ces journaux. Pour plus de détails sur la génération d'un groupe de journaux DCT, reportez-vous à l'article de la base de connaissances sur la collecte d'informations de diagnostic pour VMware View http://kb.vmware.com/kb/1017939.

Activation de la journalisation complète afin d'inclure les informations TRACE et DEBUG

Le plug-in Horizon View Agent Direct-Connection consigne les entrées de journal dans le journal standard de View Agent. Les informations TRACE et DEBUG ne sont pas incluses par défaut dans le journal.

Problème

Le plug-in Horizon View Agent Direct-Connection consigne les entrées de journal dans le journal standard de View Agent. Les informations TRACE et DEBUG ne sont pas incluses par défaut dans les journaux standard de View Agent.

Cause

La journalisation complète n'est pas activée. Vous devez activer la journalisation complète afin d'inclure les informations TRACE et DEBUG dans les journaux de View 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 à partir de View Agent et du plug-in. Recherchez `wsnm_xmlapi` pour localiser les lignes du journal du plug-in.

Lorsque View 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
```

RAM vidéo configurée insuffisante pour la machine virtuelle

La quantité de RAM vidéo configurée pour la machine virtuelle doit être suffisante.

Problème

Un écran noir apparaît lors de l'utilisation du protocole PCoIP.

Cause

La taille de la RAM vidéo configurée, de 16 Mo ou 32 Mo par exemple, est insuffisante pour la machine virtuelle.

Solution

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

Le pilote graphique installé est incorrect

La version correcte du pilote graphique d'Horizon View Agent doit être installée. Le pilote graphique a sans doute fait l'objet d'un déclassement après l'installation d'Horizon View Agent. Cela peut se produire si une version incorrecte de VMware Tools est installée après Horizon View Agent.

Problème

Un écran noir apparaît lors de l'utilisation de PCoIP suite au déclassement du pilote graphique.

Cause

La version incorrecte du pilote a été installée.

Solution

- Réinstallez Horizon View Agent.

Index