Verwaltung des Plug-In "VMware Horizon View Agent Direct-Connection"

Horizon View 5.3
View Agent 5.3

Dieses Dokument unterstützt die aufgeführten Produktversionen sowie alle folgenden Versionen, bis das Dokument durch eine neue Auflage ersetzt wird. Die neuesten Versionen dieses Dokuments finden Sie unter http://www.vmware.com/de/support/pubs.

DE-001290-00

vmware®

Die neueste technische Dokumentation finden Sie auf der VMware-Website unter:

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

Auf der VMware-Website finden Sie auch die aktuellen Produkt-Updates.

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie Ihre Kommentare und Vorschläge an:

docfeedback@vmware.com

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

VMware Global, Inc.
Zweigniederlassung Deutschland
Freisinger Str. 3
85716 Unterschleißheim/Lohhof
Germany
Tel.: +49 (0) 89 3706 17000
Fax: +49 (0) 89 3706 17333
www.vmware.com/de

Inhalt

VMware Horizon View- Verwaltung des Plug-In "Agent Direct-Connection"

Die Verwaltung des Plug-In "VMware Horizon View Agent Direct-Connection" bietet Informationen über die Installation und Konfiguration des VMware-Plug-In "Horizon View Agent Direct-Connection". Dieses Plug-In ist eine installierbare Erweiterung für View Agent, die einem View-Client die direkte Verbindung zu einem View-Desktop ohne View Connection Server ermöglicht.

Mit dem auf einem virtuellen Desktop ausgeführten Plug-In "VMware Horizon View Agent Direct-Connection" kann der Client sich direkt mit dem virtuellen Desktop verbinden. Alle Funktionen des View-Desktops wie PCoIP, HTML5 Access, RDP, USB-Umleitung und die Sitzungsverwaltung arbeiten in der gleichen Weise wie bei einer Verbindung mithilfe von View Connection Server.

Vorgesehene Zielgruppe

Diese Informationen sind für jeden gedacht, der das VMware-Plug-In "Horizon View Agent Direct-Connection" im virtuellen Desktop von VMware installieren, aktualisieren oder anwenden möchte. Der Leitfaden wurde für erfahrene Windows-Systemadministratoren geschrieben, die mit der Technologie virtueller Maschinen und mit Datacenter-Operationen vertraut sind.

Setup und Installation des VMware-Plug-In " Horizon View Agent Direct-Connection"

1

Die Installation des Plug-In "Horizon View Agent Direct-Connection" beinhaltet, dass der View-Desktop bestimmten Systemanforderungen genügt und dann das Plug-In-Installationsprogramm auf der virtuellen Maschine ausgeführt wird.

Dieses Kapitel behandelt die folgenden Themen:

Systemanforderungen für das VMware-Plug-In "Horizon View Agent Direct-Connection"

Das Plug-In "Horizon View Agent Direct-Connection" muss auf einem virtuellen View-Desktop installiert werden, der bestimmte Softwareanforderungen erfüllt.

Tabelle 1-1. Systemanforderungen für das Plug-In "Horizon View Agent Direct-Connection".

vSphere-Versionen	Betriebssystemversionen	Software
Jede vSphere-Version, die die angegebene Version von View Agent unterstützt. **Wichtig** Jeder virtuelle Desktop muss auf vSphere 5.x ESXi-Hosts gehostet werden.	Jede Betriebssystemversion, die die angegebene Version von View Agent unterstützt.	■ View Agent 5.3 oder später ■ Sie müssen Horizon View Agent nach der Installation von VMware Tools installieren.

Wichtig Jeder virtuelle View-Desktop muss mit mindestens 128 MB Video-Arbeitsspeicher konfiguriert werden, damit PCoIP korrekt funktioniert.

Der virtuelle Desktop kann einer Domäne von Microsoft Active Directory hinzugefügt werden oder Mitglied einer Workgroup sein.

Installation des VMware-Plug-In " Horizon View Agent Direct-Connection"

Sie müssen das Plug-In "Horizon View Agent Direct-Connection" auf einer virtuellen Maschine von Windows installieren, auf der View Agent ausgeführt wird.

Voraussetzungen

Bestätigen Sie, dass die virtuelle Maschine, die eine unterstützte Version von View Agent ausführt, über ausreichend konfigurierten Video-Arbeitsspeicher verfügt und eine unterstützte Version von ESXi ausführt. Siehe „Systemanforderungen für das VMware-Plug-In "Horizon View Agent Direct-Connection"“, auf Seite 7

Vorgehensweise

1 Melden Sie sich bei der virtuellen Maschine als Administrator an und führen Sie das Installationsprogramm aus, das für Ihr Betriebssystem geeignet ist.

Betriebssystem	Installationsprogramm
64-Bit-Windows	`VMware-viewagent-direct-connection-x86_64-x.y.z-nnnnnn.exe`
32-Bit-Windows	`VMware-viewagent-direct-connection-x.y.z-nnnnnn.exe`

Das Installationsprogramm bestätigt, dass die korrekte Version des Windows-Betriebssystems und View Agent installiert sind.

2 Optional geben Sie die TCP-Port-Nummer ein, die vom Plug-In für die Überwachung eingehender HTTPS-Anfragen von View-Clients im Dialogfeld für die Konfigurationsinformationen verwendet wird.

Die Standard TCP-Port-Nummer ist 443, diese sollte in den meisten Fällen nicht verändert werden. Wenn erforderlich, kann aber die Port-Nummer später nach der Installation geändert werden.

Das Kontrollkästchen **[Windows-Firewall automatisch konfigurieren]** ist standardmäßig aktiviert. Diese Auswahl fügt eine Firewall-Regel für diesen TCP-Port hinzu, um Verbindungen von View-Clients zu ermöglichen. Wenn die Windows-Firewall ausgeführt wird und diese Regel nicht erstellt wurde, ist keine Verbindung für View-Clients möglich.

Weiter

Testen Sie die komplette Installation durch den Zugriff auf diese virtuelle Maschine mithilfe von View Client. In View Client geben Sie anstelle der Festlegung des Namens oder der IP-Adresse einer Instanz des View Connection Server oder eines Sicherheitservers den Namen oder die IP-Adresse eines View-Desktops an, der dieses Plug-In ausführt. Sie authentifizieren wie gewohnt und die Benutzerführung für die Auswahl und Verbindung zu den Desktops ist dieselbe wie bei der Verbindung mithilfe von View Connection Server.

Deinstallation des VMware-Plug-In "Horizon View Agent Direct-Connection"

Sie können das Plug-In "Horizon View Agent Direct-Connection" deinstallieren wie jede andere Windows-Anwendung auch.

Vorgehensweise

1 Rufen Sie **[Systemsteuerung > Programme und Funktionen]** auf.

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

3 Wählen Sie **[Deinstallieren.]**

Das Plug-In "Horizon View Agent Direct-Connection" wird entfernt und View Agent neu gestartet.

Erweiterte Konfiguration des Plug-In "Horizon View Agent Direct-Connection"

2

Sie können die standardmäßigen Konfigurationseinstellungen für das Plug-In "Horizon View Direct-Connection" verwenden oder diese mithilfe der Gruppenrichtlinien (GPOs) des Windows Active Directory oder durch Nutzung bestimmter Windows-Registrierungseinstellungen anpassen.

Dieses Kapitel behandelt die folgenden Themen:

VMware Horizon View Einstellungen zur Konfiguration des Plug-In "Agent Direct-Connection"

Gesamtkonfiguration Die Einstellungen für das Plug-In "Horizon View Agent Direct-Connection" sind gespeichert in der lokalen Registrierung auf jedem View-Desktop. Sie können diese Einstellungen mithilfe der Gruppenrichtlinien des Active Directory von Windows (GPOs), des lokalen Richtlinieneditors oder durch direkte Bearbeitung der Registrierung verwalten.

Das Plug-In arbeitet mit den Standardwerten. Sie können diese Standardeinstellung jedoch ändern. Diese Registrierungswerte lassen sich in folgendem Registrierungsschlüssel einstellen:

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

Tabelle 2-1. Plug-In "Direct-Connection" Konfigurationseinstellungen

Einstellung	Registrierungswert	Typ	Beschreibung
HTTPS-Port-Nummer (HTTPS Port Number)	httpsPortNumber	REG_SZ	TCP-Port-Nummer für das Plug-In für eingehende HTTPS-Anfragen von View Client. Wird dieser Wert geändert, müssen Sie eine entsprechende Änderung für die Windows-Firewall durchführen, damit der neue Wert zugelassen ist.
Zeitüberschreitung der Sitzung (Session Timeout)	sessionTimeout	REG_SZ	Zeitspanne, die einem Benutzer für eine Sitzung nach der Anmeldung in View Client zur Verfügung steht. Der Wert wird in Minuten festgelegt. Wenn diese Richtlinie nicht konfiguriert oder deaktiviert ist, beträgt der Standardwert 600 Minuten. Wenn die Zeit für eine Desktopsitzung abgelaufen ist, wird die Sitzung beendet und die Verbindung vom Desktop zu View Client getrennt.

Tabelle 2-1. Plug-In "Direct-Connection" Konfigurationseinstellungen (Fortsetzung)

Einstellung	Registrierungswert	Typ	Beschreibung
Ausschlussklausel aktiviert (Disclaimer Enabled)	disclaimerEnabled	REG_SZ	Der Wert wird eingestellt auf `TRUE` oder `FALSE`. Beträgt die Einstellung `TRUE`, wird der Text für die Ausschlussklausel zur Benutzerbestätigung bei der Anmeldung angezeigt. Der Text wird, wenn vorhanden, angezeigt aus 'Text Ausschlussklausel' oder von der GPO `Configuration\Windows Settings\Security Settings\Local Policies\Security Options: Interaktive Anmeldung`. Die Standardeinstellung für disclaimerEnabled ist `FALSE`.
Text Ausschlussklausel (Disclaimer Text)	disclaimerText	REG_SZ	Der Text für die Ausschlussklausel wird für Benutzer von View Client bei der Anmeldung angezeigt. Die Richtlinie für die Aktivierung der Ausschlussklausel muss auf `TRUE` eingestellt sein. Wenn kein Text festgelegt ist, wird als Standardwert der Wert von der Windows-Richtlinie `Configuration\Windows Settings\Security Settings\Local Policies\Security Options` verwendet.
Client-Einstellung: Immer verbinden (AlwaysConnect)	alwaysConnect	REG_SZ	Der Wert wird eingestellt auf `TRUE` oder auf `FALSE`. Die Einstellung für AlwaysConnect wird an View Client gesendet. Ist diese Richtlinie auf `TRUE` eingestellt, werden dadurch alle gespeicherten Client-Einstellungen überschrieben. Standardmäßig ist kein Wert angegeben. Die Aktivierung dieser Richtlinie legt den Wert `TRUE` fest. Die Deaktivierung dieser Richtlinie führt zum Wert `FALSE`.
Externer PCoIP-Port (External PCoIP Port)	externalPCoIPPort	REG_SZ	Die Port-Nummer, die an View Client für die Ziel-TCP/UDP-Port-Nummer gesendet wird, die für das PCoIP-Protokoll verwendet wird. Ein +- Zeichen vor der Nummer gibt eine relative Port-Nummer in Bezug auf die Port-Nummer an, die für HTTPS verwendet wird. Dieser Wert muss nur eingestellt werden, wenn die extern vorhandene Port-Nummer nicht dem Port entspricht, den der Dienst benutzt. Typischerweise befindet sich diese Port-Nummer in einer NAT-Umgebung. Standardmäßig ist kein Wert angegeben.
Externer Blast-Port (External Blast Port)	externalBlastPort	REG_SZ	Die Port-Nummer, die an View Client für die Ziel-TCP-Port-Nummer gesendet wird, die für das HTML5/Blast-Protokoll verwendet wird. Ein +- Zeichen vor der Nummer gibt eine relative Port-Nummer in Bezug auf die Port-Nummer an, die für HTTPS verwendet wird. Dieser Wert muss nur eingestellt werden, wenn die extern vorhandene Port-Nummer nicht dem Port entspricht, den der Dienst benutzt. Typischerweise befindet sich diese Port-Nummer in einer NAT-Umgebung. Standardmäßig ist kein Wert angegeben.
Externer RDP-Port (External RDP Port)	externalRDPPort	REG_SZ	Die Port-Nummer, die an View Client für die Ziel-TCP-Port-Nummer gesendet wird, die für das RDP-Protokoll verwendet wird. Ein +-Zeichen vor vor der Nummer gibt eine relative Port-Nummer in Bezug auf die Port-Nummer an, die für HTTPS verwendet wird. Dieser Wert muss nur eingestellt werden, wenn die extern offen Port-Nummer nicht dem Port entspricht, den der Dienst benutzt. Typischerweise befindet sich diese Port-Nummer in einer NAT-Umgebung. Standardmäßig ist kein Wert angegeben.

Tabelle 2-1. Plug-In "Direct-Connection" Konfigurationseinstellungen (Fortsetzung)

Einstellung	Registrierungswert	Typ	Beschreibung
Externe IP-Adresse (External IP Address)	externalIPAddress	REG_SZ	Die IP v4-Adresse, die an View Client für die Ziel-IP-Adresse gesendet wird, die für sekundäre Protokolle (RDP, PCoIP, Framework-Kanal usw.) verwendet wird. Dieser Wert muss nur eingestellt werden, wenn die extern vorhandene Adresse nicht der Adresse des Desktopcomputers entspricht. Typischerweise befindet sich diese Adresse in einer NAT-Umgebung. Standardmäßig ist kein Wert angegeben.
Externer Framework-Kanal-Port	externalFramework-ChannelPort	REG_SZ	Die Port-Nummer, die an den View.Client für die Ziel-TCP-Port-Nummer gesendet wird, die für das Framework-Kanal-Protokoll verwendet wird. Ein +-Zeichen vor der Nummer gibt eine relative Port-Nummer in Bezug auf die Port-Nummer an, die für HTTPS verwendet wird. Dieser Wert muss nur eingestellt werden, wenn die extern vorhandene Port-Nummer nicht dem Port entspricht, den der Dienst benutzt. Typischerweise befindet sich diese Port-Nummer in einer NAT-Umgebung. Standardmäßig ist kein Wert angegeben.
USB aktiviert (USB Enabled)	usbEnabled	REG_SZ	Der Wert wird eingestellt auf `TRUE` oder auf `FALSE`. Legt fest, ob Desktops USB- Geräte benutzen können, die mit dem Client-System verbunden sind. Der Standardwert ist aktiviert. Wenn Sie aus Sicherheitsgründen die Verwendung externer Geräte unterbinden möchten, ändern Sie die Einstellung in deaktiviert (`FALSE`).
Client-Einstellung: USB automatische Verbindung (USB AutoConnect)	usbAutoConnect	REG_SZ	Der Wert wird eingestellt auf `TRUE` oder auf `FALSE`. Verbindet USB-Geräte mit dem Desktop, wenn diese eingesteckt sind. Ist diese Richtlinie aktiviert, wird jede gespeichert Client-Einstellung überschrieben. Standardmäßig ist kein Wert angegeben.
Zurücksetzen aktiviert (Reset Enabled)	resetEnabled	REG_SZ	Der Wert wird eingestellt auf `TRUE` oder auf `FALSE`. Ist die Einstellung `TRUE`, kann ein authentifizierter View-Client einen Neustart auf Betriebssystemebene durchführen. Diese Einstellung ist standardmäßig deaktiviert (`FALSE`).
Zeitüberschreitung für Cache der Client-Zugangsdaten (Client Credential Cache Timeout)	clientCredentialCache-Timeout	REG_SZ	Zeit in Minuten, die ein View-Client einem Benutzer zur Verfügung stellt, um ein gespeichertes Kennwort zu benutzen. 0 bedeutet nie und -1 immer. View Client bietet Benutzern die Möglichkeit, ihre Kennwörter zu speichern, wenn diese Einstellung auf einen gültigen Wert festgelegt ist. Der Standardwert lautet 0 Minuten (nie).

Einstellungen für View Client ändern nicht das Verhalten des Plug-In. Diese Einstellungen werden an View Client zur Auswertung gesendet.

Die externen Port-Nummern und die Werte für die externen IP-Adressen werden für die Unterstützung von NAT (Network Address Translation) und die Port-Zuordnung verwendet. Weitere Informationen finden Sie unter „Verwendung von Netzwerkadressübersetzung und Portzuordnung“, auf Seite 15.

Sie können mithilfe des lokalen Richtlinieneditors (Local Policy Editor) oder durch Verwendung von GPOs (Group Policy Objects, Gruppenrichtlinienobjekte) im Active Directory Richtlinien festlegen, die diese Einstellungen überschreiben. Einstellungen für Richtlinien haben Vorrang vor herkömmlichen Registrierungseinstellungen. Eine GPO-Vorlage wird zur Konfiguration der Richtlinien zur Verfügung gestellt. Wenn View Agent und das Plug-In im Standardverzeichnis installiert sind, befindet sich die Vorlagendatei in folgendem Verzeichnis:

```
C:\Programme\ VMware\VMware View\Agent\extras\view_agent_direct_connection.adm
```

Sie können diese Vorlagendatei in das Active Directory importieren oder mit dem Local Group Policy Editor (Editor für lokale Gruppenrichtlinien) die Verwaltung dieser Konfigurationseinstellungen vereinfachen. Unter dem Microsoft-Richtlinieneditor und in der GPO-Dokumentation finden Sie Einzelheiten zur Handhabung der Richtlinieneinstellungen in dieser Form. Richtlinieneinstellungen für das Plug-In werden in folgendem Registrierungsschlüssel gespeichert.

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

Deaktivieren der schwachen Verschlüsselung in SSL/TLS

Sie können festlegen, dass für View Client bei der View-Desktop-Kommunikation, die das SSL/TLS-Protokoll verwendet, keine weiche Verschlüsselung zulässig ist durch Nutzung des Schutzverfahrens dieses View-Desktops.

Die Konfiguration für das Deaktivieren der schwachen Verschlüsselung wird in der Windows-Registrierung gespeichert. Eine Änderung dieser Einstellungen muss für alle Desktop-Systeme erfolgen, auf denen das Plug-In "View Agent Direct-Connection" ausgeführt wird.

HINWEIS Diese Einstellungen beeinflussen die gesamte Nutzung von SSL/TLS im Betriebssystem.

Sowohl SSL 3.0 wie auch TLS 1.0 (RFC2246) mit INTERNET-DRAFT `56-bit Export Cipher Suites For TLS draft-ietf-tls-56-bit-ciphersuites-00.txt` bieten Möglichkeiten zur Nutzung unterschiedlicher Verschlüsselungsmethoden. Die einzelne Verschlüsselungsmethode legt den Schlüsselaustausch, die Authentifizierung, die Chiffrierung und die MAC-Algorithmen fest, die in einer SSL/TLS-Sitzung genutzt werden.

Voraussetzungen

Voraussetzung ist eine gewisse Erfahrung bei der Bearbeitung der Windows-Registrierungsschlüssel mit dem Registrierungseditor `Regedt32.exe`.

Vorgehensweise

- Starten Sie den Registrierungseditor `Regedt32.exe` und gehen Sie zu diesem Registrierungsschlüssel:`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL`

Weiter

Tabelle 2-2. Aktualisierung der Verschlüsselungsmethoden

Windows XP SP3	Windows Vista und später
1 Im Unterschlüssel `\Ciphers\DES 56/56` fügen Sie einen DWORD-Wert `Enabled` mit einem Wert von `0x0` hinzu. 2 Im Unterschlüssel `\Hashes\MD5` fügen Sie einen DWORD-Wert `Enabled` mit einem Wert von `0x0` hinzu. Diese Aktualisierungen stellen sicher, dass nur die folgenden Verschlüsselungen unter Windows XP SP3 verfügbar sind: ■ SSLv3 168 Bits DES-CBC3-SHA ■ SSLv3 128 Bits RC4-SHA ■ TLSv1 168 Bits DES-CBC3-SHA ■ TLSv1 128 Bits RC4-SHA	1 Im Unterschlüssel `\Hashes` erstellen Sie einen Unterschlüssel `MD5`. 2 Im Unterschlüssel `\Hashes\MD5` fügen Sie einen DWORD-Wert `Enabled` mit einem Wert von `0x0` hinzu. Diese Aktualisierungen stellen sicher, dass nur die folgenden Verschlüsselungen unter Windows XP Vista verfügbar sind: ■ 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

Ersetzen des selbstsignierten SSL Server-Standardzertifikats

Ein selbstsigniertes SSL Server-Zertifikat schützt View Client nicht ausreichend gegen Gefährdungen durch Fälschen und Abhören. Um Ihre Desktops gegen diese Bedrohungen abzusichern, müssen Sie das erstellte selbstsignierte Zertifikat ersetzen.

Wenn das Plug-In "View Agent Direct-Connection" das erste Mal nach der Installation gestartet wird, erstellt es automatisch ein selbstsigniertes SSL Server-Zertifikat und platziert es im Windows-Zertifikatsspeicher. Das SSL Server-Zertifikat wird View Client während der SSL-Protokollverhandlungen zur Verfügung gestellt, um dem Client Informationen über diesen View-Desktop zu liefern. Das selbstsignierte SSL Server-Standardzertifikat kann nicht für diesen Desktop garantieren, solange es nicht durch ein Zertifikat ersetzt wird, das von einer Zertifizierungsstelle (CA, Certificate Authority) signiert wurde, der der Client vertraut und die komplett durch die Zertifikatsüberprüfungen von View Client bestätigt wurde.

Das Verfahren für das Speichern dieses Zertifikats im Windows-Zertifikatsspeicher und das Verfahren für dessen Ersetzung mit einem ordnungsgemäßen CA-Signierten Zertifikat sind dieselben, die für View Connection Server (Version 5.1 oder später) verwendet werden. Unter "Konfigurieren von SSL-Zertifikaten für View-Server" im Installationshandbuch von VMware Horizon View finden Sie weitere Erläuterungen zum Ersetzen von Zertifikaten.

Es werden Zertifikate mit SAN (Subject Alternative Name, Alternativer Antragstellername) und Wildcard-Zertifikate unterstützt.

Hinweis Um CA-signierte SSL Server-Zertifikate einer großen Anzahl von View-Desktops mithilfe des Plug-In "View Agent Direct-Connection" zuzuordnen, verwenden Sie das Active Directory, um diese Zertifikate an jede virtuelle Maschine zu verteilen. Weitere Informationen finden Sie unter: http://technet.microsoft.com/en-us/library/cc732625.aspx

---

Autorisierung von View Client für den Zugriff auf den View-Desktop

Das Autorisierungsverfahren, das es einem Benutzer von View Client ermöglicht, direkt auf den View-Desktop zuzugreifen, wird innerhalb einer lokalen Betriebssystemgruppe namens **[Benutzer von "View Agent Direct-Connection"]** ausgeführt.

Ist ein Benutzer ein Mitglied dieser Gruppe, hat er die Berechtigung, sich direkt mit dem Desktop zu verbinden. Wenn das Plug-In zuvor installiert wurde, wird diese lokale Gruppe erstellt, die die Gruppe 'Authentifizierte Benutzer' enthält. Jeder, der durch dieses Plug-In erfolgreich authentifiziert wurde, ist zum Zugriff auf den Desktop berechtigt.

Um den Zugriff auf diesen Desktop zu beschränken, können Sie die Mitgliedschaft dieser Gruppe verändern und eine Liste von Benutzern und Benutzergruppen festlegen. Bei diesen Benutzern kann es sich um lokale oder um Domänenbenutzer und -benutzergruppen handeln. Ist der Benutzer von View Client nicht in dieser Gruppe enthalten, erhält der Benutzer nach der Authentifizierung eine Meldung, dass er nicht zum Zugriff auf diesen Desktop berechtigt ist.

Verwendung von Netzwerkadressübersetzung und Portzuordnung

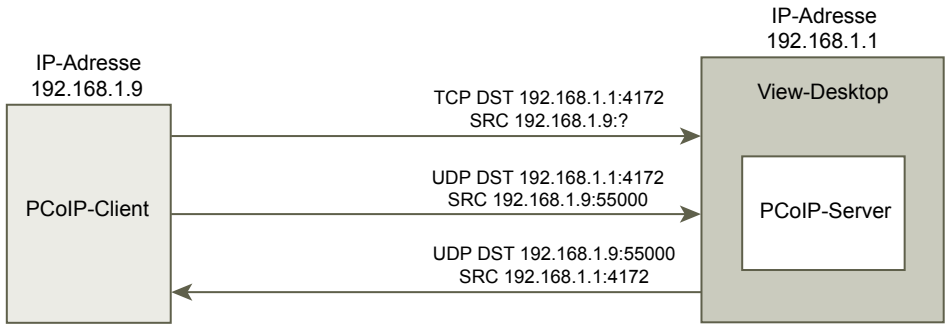
Netzwerkadressübersetzung (NAT) und Konfiguration der Portzuordnung sind erforderlich, wenn View Client-Instanzen mit View-Desktops in verschiedenen Netzwerken verbunden werden.

In den hier aufgeführten Beispielen müssen Sie externe Adressierungsinformationen auf dem View-Desktop konfigurieren, sodass View Client diese Informationen zur Verbindung mit dem View-Desktop über NAT oder ein Portzuordnungsgerät verwenden kann. Diese URL ist identisch mit den Einstellungen „Externe URL“ und „PCoIP - Externe URL“ auf View Connection Server und Sicherheitsserver.

Wenn View Client sich in einem anderen Netzwerk befindet und ein NAT-Gerät sich zwischen View Client und dem virtuellen View-Desktop befindet, auf dem das Plug-In ausgeführt wird, ist ein NAT oder eine Portzuordnungskonfiguration erforderlich. Wenn sich z. B. zwischen View Client und dem virtuellen View-Desktop eine Firewall befindet, fungiert sie als NAT- oder Portzuordnungsgerät.

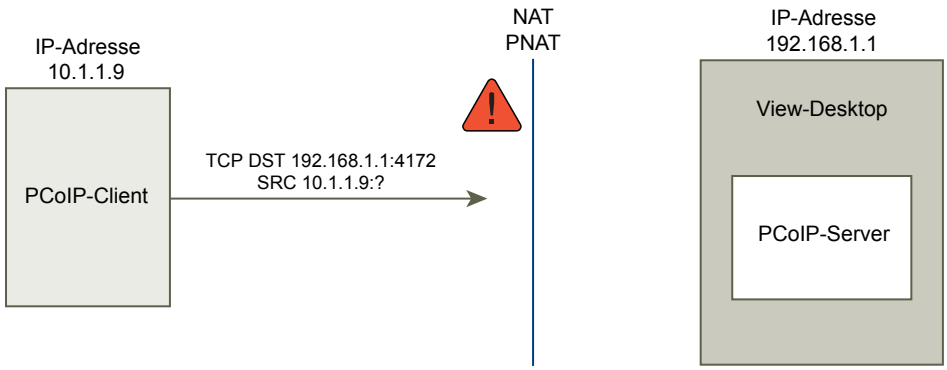
Eine Beispielbereitstellung eines View-Desktops, dessen IP-Adresse 192.168.1.1 lautet, veranschaulicht die Konfiguration von NAT und Portzuordnung. Ein View Client-System mit der IP-Adresse 192.168.1.9 in demselben Netzwerk richtet eine PCoIP-Verbindung mittels TCP und UDP ein. Es handelt sich dabei um eine direkte Verbindung ohne NAT oder Portzuordnungskonfiguration.

Abbildung 2-1. Direktes PCoIP von einem Client aus demselben Netzwerk



Wenn Sie ein NAT-Gerät zwischen Client und Desktop hinzufügen, sodass sie in unterschiedlichen Adressbereichen betrieben werden, und keine Konfigurationsänderungen an dem Plug-In vornehmen, werden die PCoIP-Pakete nicht richtig weitergeleitet und schlagen fehl. In diesem Beispiel verwendet der Client einen anderen Adressbereich und hat die IP-Adresse 10.1.1.9. Diese Einrichtung misslingt, weil der Client die Adresse des Desktops verwendet, um die TCP- und UDP-PCoIP-Pakete zu senden. Die Zieladresse 192.168.1.1 ist vom Clientnetzwerk aus nicht nutzbar und könnte dazu führen, dass ein leerer Clientbildschirm angezeigt wird.

Abbildung 2-2. PCoIP von einem Client über das NAT-Gerät – Darstellung des Fehlers

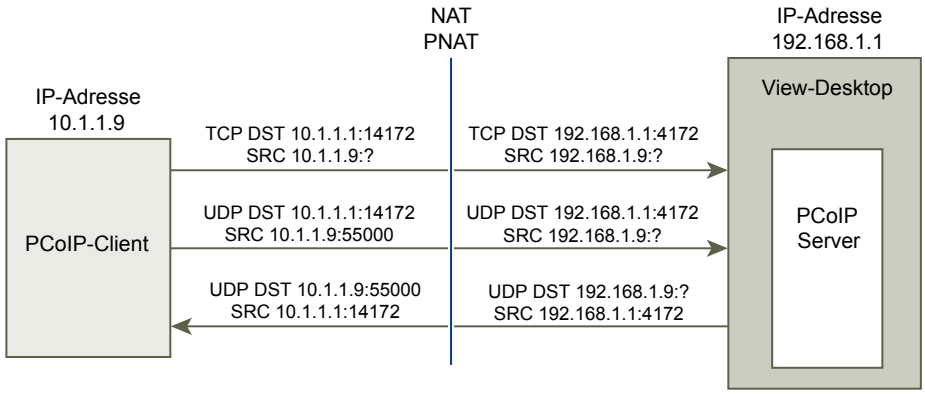


Zur Lösung dieses Problems müssen Sie das Plug-In zur Verwendung einer externen IP-Adresse konfigurieren. Wenn `externalIPAddress` für diesen Desktop mit 10.1.1.1 konfiguriert ist, erhält der Client vom Plug-In die IP-Adresse 10.1.1.1, wenn Desktop-Protokollverbindungen zum Desktop hergestellt werden. Für PCoIP muss der PCoIP Secure Gateway-Service für diese Einrichtung auf dem Desktop gestartet werden.

Was die Portzuordnung betrifft: Wenn der Desktop den standardmäßigen PCoIP-Port 4172 verwendet, muss der Client einen anderen Zielport verwenden, der Port 4172 am Portzuordnungsgerät zugeordnet ist. Sie müssen das Plug-In für diese Einrichtung konfigurieren. Wenn das Portzuordnungsgerät Port 14172 4172 zuordnet, muss der Client den Zielport 14172 für PCoIP verwenden. Sie müssen diese Einrichtung für PCoIP konfigurieren. Setzen Sie `externalPCoIPPort` im Plug-In auf 14172.

In einer Konfiguration, die NAT und Portzuordnung verwendet, und wo `externalIPAdress` auf 10.1.1.1 gesetzt ist, was der Netzwerkübersetzung 192.168.1.1 entspricht, und `externalPColPPort` auf 14172 gesetzt ist, was der Portzuordnung 4172 entspricht.

Abbildung 2-3. PCoIP von einem Client über ein NAT-Gerät und Portzuordnung



Wie bei der TCP/UDP-Portkonfiguration für PCoIP mit externem PCoIP müssen Sie, wenn für den RDP-Port (3389) oder Framework-Kanal-Port (32111) eine Portzuordnung besteht, `externalRDPPort` und `externalFrameworkChannelPort` konfigurieren, um die TCP-Portnummern festzulegen, die der Client verwendet, um diese Verbindungen über ein Portzuordnungsgerät herzustellen.

Erweitertes Adressierungsschema

Wenn Sie verschiedene View-Desktops so konfigurieren möchten, dass auf diese über ein NAT und ein Port-Zuordnungsgerät über dieselbe externe IP-Adresse zugegriffen werden kann, müssen Sie jedem View-Desktop ein eindeutiges Set an Port-Nummern zuweisen. Die Clients können dann dieselbe Ziel-IP-Adresse nutzen, aber gleichzeitig eine eindeutige TCP-Port-Nummer für die HTTPS-Verbindung verwenden, um die Verbindung einem bestimmten virtuellen Desktop zuzuordnen.

Beispiele für Adressierungsschemata

In diesem Beispiel wird der HTTPS-Port 1000 einem Desktop zugeordnet und der HTTPS-Port 1005 einem anderen, wobei beide dieselbe Ziel-IP-Adresse nutzen. In diesem Fall würde die Konfiguration einzelner eindeutiger externer Port-Nummern für jeden View-Desktop für die Desktop-Protokollverbindungen zu komplex werden. Deshalb können die Plug-In-Einstellungen `externalPCoIPPort`,`externalRDPPort` und `externalFrameworkChannelPort` einen optionalen relationalen Ausdruck anstelle eines festen Werts annehmen, um eine Port-Nummer relativ zu der vom Client verwendeten Basis-HTTPS-Port-Nummer zu definieren.

Wenn das Port-Zuordnungsgerät die Port-Nummer 1000 für HTTPS verwendet, zugeordnet zu TCP 443, die Port-Nummer 1001 für RDP, zugeordnet zu TCP 3389, die Port-Nummer 1002 für PCoIP, zugeordnet zu TCP und UDP 4172, sowie die Port-Nummer 1003 für den Framework-Kanal, zugeordnet zu TCP 32111, können die externen Port-Nummern zur Vereinfachung der Konfiguration in dern Form `externalRDPPort=+1`, `externalPCoIPPort=+2` and `externalFrameworkChannelPort=+3` konfiguriert werden. Stammt die HTTPS-Verbindung von einem Client, der eine HTTPS-Ziel-Port-Nummer von 1000 verwendet hat, dann werden die externen Port-Nummern automatisch berechnet und zwar relativ zu dieser Port-Nummer von 1000 in der Form 1001, 1002 bzw. 1003.

Für die Bereitstellung eines anderen virtuellen Deskotps ergibt sich folgende Situation: Wenn das Port-Zuordnungsgerät die Port-Nummer 1005 für HTTPS verwendet, zugeordnet zu TCP 443, die Port-Nummer 1006 für RDP, zugeordnet zu TCP 3389, die Port-Nummer 1007 für PCoIP, zugeordnet zu TCP und UDP 4172, sowie Port-Nummer 1008 für den Framework-Kanal, zugeordnet zu TCP 32111, mit genau derselben externen Port-Konfiguration auf dem Desktop (+1, +2, +3 usw.) und wenn die HTTPS-Verbindung von einem Client stammt, der eine HTTPS-Ziel-Port-Nummer von 1005 verwendet, werden die externe Port-Nummern automatisch berechnet und zwar relativ zu dieser Port-Nummer 1005 in der Form 1006, 1007 bzw. 1008.

Dieses Schema bietet allen View-Desktops die Möglichkeit, identisch konfiguriert zu werden und dabei alle dieselbe externe IP-Adresse zu verwenden. Die Zuordnung von Port-Nummern in Fünfer-Schritten (1000, 1005, 1010 …) für die HTTPS-Basis-Port-Nummer ermöglicht deshalb den Zugriff auf über 12.000 virtuelle Desktops über dieselbe IP-Adresse. und verwenden Sie die Basis-Port-Nummer, um den virtuellen Desktop zu bestimmen und die Verbindung dazu auf der Basis der Konfiguration des Port-Zuordnungsgerätes aufzubauen. Für `externalIPAddress`=10.20.30.40, `externalRDPPort`=+1, `externalPCoIPPort`=+2 und `externalFrameworkChannelPort`=+3, konfiguriert für alle virtuelle Desktops, erfolgt die Zuordnung zu den virtuellen Desktops wie in der NAT und der Port-Zuordnungstabelle beschrieben.

Tabelle 2-3. NAT und Port-Zuordnungswerte

VM#	Desktop-IP-Adresse	HTTPS	RDP	PCOIP (TCP und UDP)	Framework-Kanal
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 verbindet dann zur IP-Adresse 10.20.30.40 und einer HTTPS-Ziel-Port-Nummer von (1000 + *n* * 5), wobei *n* die View-Desktop-Nummer darstellt. Um mit dem View-Desktop 3 zu verbinden, muss der Client dann eine Verbindung zu 10.20.30.40:1015 herstellen. Dieses Adressierungsschema vereinfacht die Konfiguration für jeden View-Desktop erheblich. Alle Desktops werden mit identischen externen Adressen und Port-Konfigurationen konfiguert. Die NAT- und Port-Zuordnungskonfiguration wird innerhalb der NAT und des Port-Zuordnungsgeräts mit diesem einheitlichen Muster durchgeführt und auf alle View-Desktops kann über eine einzige öffentliche IP-Adresse zugegriffen werden. Der Client verwendet typischerweise einen einzigen öffentlichen DNS-Namen, der zu dieser IP-Adresse führt.

Problembehandlung für das VMware-Plug-In " Horizon View Agent Direct-Connection"

3

Bei der Anwendung des Plug-In "Horizon View Agent Direct-Connection" können bekannte Probleme auftreten, die behoben werden müssen.

Wenn ein Problem mit dem Plug-In "Horizon View Agent Direct-Connection" auftritt, vergewissern Sie sich, dass die korrekte Version installiert ist und ausgeführt wird. Im obigen Beispiel sind die Versionsdaten des Plug-In `version=e.x.p build-855808, buildtype=release`. Der Plug-In-Name "VMware View Agent XML API Handler Plugin" wird aufgezeichnet.

Um ein Support-Problem mit VMware behandeln zu können, müssen Sie immer die komplette Protokollierung aktivieren, das Problem reproduzieren und ein DCT-Protokoll-Set (Data Collection Tool, Datenerfassungstool) erstellen. Der technische Support von VMWare ist dann in der Lage, diese Protokolle auszuwerten. Erläuterungen zur Erstellung eines DCT-Protokoll-Sets erhalten Sie im View-KB-Artikel "Zusammenstellung von Diagnoseinformationen für VMware" http://kb.vmware.com/kb/1017939.

Aktivieren der vollständigen Protokollierung zur Aufnahme der TRACE- und DEBUG-Informationen

Das Plug-In "Horizon View Agent Direct-Connection" schreibt Protokolleinträge in das Standardprotokoll von View Agent. Die TRACE- und DEBUG-Informationen sind standardmäßig darin nicht enthalten.

Problem

Das Plug-In "Horizon View Agent Direct-Connection" schreibt Protokolleinträge in das Standardprotokoll von View Agent. Die TRACE- und DEBUG-Informationen sind standardmäßig darin nicht enthalten.

Ursache

Die vollständige Protokollierung ist nicht aktiviert. Um die TRACE- und DEBUG-Informationen in die Protokolle von View Agent aufzunehmen, müssen Sie die komplette Protokollierung aktivieren.

Lösung

1 Öffnen Sie eine Befehlseingabezeile und führen Sie `C:\Programme\VMware\VMware View\Agent\DCT\support.bat loglevels` aus

2 Geben Sie **3** für eine vollständige Protokollierung ein.

Die Debug-Protokolldateien sind in `%ALLUSERSPROFILE%\VMware\VDM\logs` enthalten. Die Datei `debug*.log` enthält von View Agent und dem Plug-In protokollierte Informationen. Suchen Sie nach `wsnm_xmlapi` für die Plug-In-Protokollzeilen.

Wenn View Agent gestartet ist, wird die Plug-In-Version protokolliert:

```
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
```

Unzureichender für die virtuelle Maschine konfigurierter Video-Arbeitsspeicher

Für die virtuelle Maschine muss ausreichend Video-Arbeitsspeicher konfiguriert werden.

Problem

Ein schwarzer Bildschirm wird dargestellt, wenn PCoIP verwendet wird.

Ursache

Es wurde ein nicht ausreichender Video-Arbeitsspeicher von etwa 16 MB oder 32 MB für die virtuelle Maschine konfiguriert.

Lösung

- Legen Sie mindestens 128 MB Video-Arbeitsspeicher für jede virtuelle Maschine fest.

Ein falscher Grafiktreiber wurde installiert

Die korrekte Version des Grafiktreibers von Horizon View Agent muss installiert sein. Der Grafiktreiber wurde eventuell nach der Installation von Horizon View Agent heruntergestuft. Dies kann daran liegen, dass eine falsche Version von VMware Tools nach Horizon View Agent installiert wurde.

Problem

Ein schwarzer Bildschirm wird dargestellt, wenn PCoIP wegen eines heruntergestuften Grafiktreibers verwendet wird.

Ursache

Die falsche Version des Grafiktreibers wurde installiert.

Lösung

- Installieren Sie Horizon View Agent erneut.

Index