

Verwaltung des Plug-Ins „View Agent Direct- Connection“

Geändert am 13. Dezember 2018
VMware Horizon 7 7.7



vmware®

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

<https://docs.vmware.com/de/>

Die VMware-Website enthält auch die neuesten Produkt-Updates.

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie diese an:

docfeedback@vmware.com

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

VMware Global, Inc.
Zweigniederlassung Deutschland
Willy-Brandt-Platz 2
81829 München
Germany
Tel.: +49 (0) 89 3706 17 000
Fax: +49 (0) 89 3706 17 333
www.vmware.com/de

Inhalt

Verwaltung des Plug-Ins „View Agent Direct-Connection“	4
1 Installation des Plug-Ins „View Agent Direct-Connection“	5
Systemanforderungen für das Plug-In „View Agent Direct-Connection“	5
Installieren des Plug-Ins „View Agent Direct-Connection“	5
Unbeaufsichtigte Installation des Plug-Ins „View Agent Direct-Connection“	6
2 Erweiterte Konfiguration des Plug-Ins „View Agent Direct-Connection“	8
Konfigurationseinstellungen des Plug-Ins „View Agent Direct-Connection“	8
Deaktivieren von schwachen Verschlüsselungen in SSL/TLS	11
Ersetzen des standardmäßigen selbstsignierten TLS-Serverzertifikats	12
Autorisierung von Horizon Client für den Zugriff auf Desktops und Anwendungen	13
Verwenden der Netzwerkadressübersetzung (NAT) und Portzuordnung	13
Hinzufügen einer Zertifizierungsstelle zum Windows-Zertifikatspeicher	17
3 Einrichten von HTML Access	18
Installieren von Horizon 7 Agent für HTML Access	18
Einrichten der statischen Inhaltsübermittlung	19
Einrichten eines von einer vertrauenswürdigen Zertifizierungsstelle signierten TLS-Serverzertifikats	20
Deaktivieren des HTTP/2-Protokolls auf Windows 10- und Windows 2016-Desktops	21
4 Einrichten von VADC (View Agent Direct Connection) auf Remote-Desktop-Dienste-Hosts	22
RDS-Hosts	22
Berechtigungen für veröffentlichte Desktops und Anwendungen	23
5 Fehlerbehebung des Plug-Ins „View Agent Direct-Connection“	24
Falsche Grafikhardware wurde installiert	24
Nicht genügend Video-RAM	25
Aktivieren der vollständigen Protokollierung für das Einbeziehen von TRACE- und DEBUG-Informationen	25

Verwaltung des Plug-Ins „View Agent Direct-Connection“

Administration des View Agent Direct-Connection-Plug-Ins bietet Informationen zur Installation und Konfiguration des View Agent Direct-Connection-Plug-Ins. Dieses Plug-In ist eine installierbare Erweiterung für Horizon Agent, um einem Horizon Client ohne Verbindungsserver eine direkte Verbindung zu einem VM-basierten Desktop, einem veröffentlichten Desktop oder einer Anwendung zu ermöglichen. Alle Desktop- und Anwendungsfunktionen funktionieren auf dieselbe Weise wie bei der Verbindung des Benutzers über den Verbindungsserver.

Zielgruppe

Diese Informationen richten sich an einen Administrator, der das Plug-In „View Agent Direct-Connection“ in einem VM-basierten Desktop oder einem RDS-Host installieren, aktualisieren und konfigurieren möchte. Dieses Handbuch wurde für erfahrene Windows-Systemadministratoren verfasst, die mit der Technologie virtueller Maschinen sowie mit Datencenter-Vorgängen vertraut sind.

Installation des Plug-Ins „View Agent Direct-Connection“

1

Das Plug-In „View Agent Direct-Connection“ (VADC) aktiviert Horizon Clients, um eine direkte Verbindung zu VM-basierten Desktops, veröffentlichten Desktops oder Anwendungen herzustellen. Das VADC-Plug-In ist eine Erweiterung von Horizon 7 Agent und wird auf VM-basierten Desktops oder RDS-Hosts installiert.

Dieses Kapitel enthält die folgenden Themen:

- [Systemanforderungen für das Plug-In „View Agent Direct-Connection“](#)
- [Installieren des Plug-Ins „View Agent Direct-Connection“](#)
- [Unbeaufsichtigte Installation des Plug-Ins „View Agent Direct-Connection“](#)

Systemanforderungen für das Plug-In „View Agent Direct-Connection“

Das VADC-Plug-In (View Agent Direct-Connection) ist auf Computern installiert, auf denen Horizon 7 Agent bereits installiert ist. Eine Liste der Betriebssysteme, die Horizon 7 Agent unterstützt, finden Sie unter „Unterstützte Betriebssysteme für Horizon Agent“ im Dokument *Horizon 7-Installation*.

Das VADC-Plug-In hat folgende zusätzliche Anforderungen:

- Die virtuelle oder physische Maschine, auf der das VADC-Plug-In installiert ist, muss mindestens 128 MB Video-RAM aufweisen, damit PCoIP ordnungsgemäß funktioniert.
- Bei einer virtuellen Maschine müssen Sie die VMware Tools vor der Installation von Horizon 7 Agent installieren.

Hinweis Ein Desktop auf Basis einer virtuellen Maschine, der VADC unterstützt, kann einer Microsoft Active Directory-Domäne beitreten oder Mitglied einer Arbeitsgruppe sein.

Installieren des Plug-Ins „View Agent Direct-Connection“

Das VADC-Plug-In (View Agent Direct-Connection) ist in einer Windows Installer-Datei verpackt, die Sie von der VMware Website herunterladen und installieren können.

Voraussetzungen

- Stellen Sie sicher, dass Horizon 7 Agent installiert ist. Wenn in Ihrer Umgebung Horizon 7-Verbindungsserver nicht vorhanden ist, installieren Sie Horizon 7 Agent über die Befehlszeile und legen Sie einen Parameter fest, der Horizon 7 Agent veranlasst, sich nicht beim Horizon 7-Verbindungsserver zu registrieren. Siehe [Installieren von Horizon 7 Agent für HTML Access](#).
- Aktivieren Sie die Bildschirm-DMA-Einstellung für virtuelle Maschinen auf vSphere 6.0 und höher. Wenn die Bildschirm-DMA-Einstellung deaktiviert ist, sehen die Benutzer beim Herstellen einer Verbindung mit dem Remote-Desktop einen schwarzen Bildschirm. Weitere Informationen zur Einstellung der Bildschirm-DMA-Funktion finden Sie im VMware-Knowledgebase-Artikel 2144475 <http://kb.vmware.com/kb/2144475>.

Verfahren

- 1 Laden Sie die Installationsdatei des VADC-Plug-Ins von der VMware-Downloadseite unter <http://www.vmware.com/go/downloadview> herunter.

Der Dateiname des Installationsprogramms lautet VMware-viewagent-direct-connection-x86_64-y.y.y-xxxxxx.exe für 64-Bit-Windows oder VMware-viewagent-direct-connection--y.y.y-xxxxxx.exe für 32-Bit-Windows, wobei y.y.y die Versionsnummer und xxxxxx die Build-Nummer ist.
- 2 Doppelklicken Sie auf die Installationsdatei.
- 3 (Optional) Ändern Sie die TCP-Portnummer.

Die standardmäßige Portnummer lautet 443.
- 4 (Optional) Wählen Sie Konfigurationsoptionen für den Windows-Firewall-Dienst aus.

Standardmäßig wird **Windows-Firewall automatisch konfigurieren** ausgewählt, und das Installationsprogramm konfiguriert die Windows-Firewall, damit die erforderlichen Netzwerkverbindungen möglich werden.
- 5 (Optional) Entscheiden Sie, ob Sie SSL 3.0 deaktivieren möchten.

Standardmäßig ist **Unterstützung für SSLv3 automatisch deaktivieren (empfohlen)** ausgewählt und das Installationsprogramm deaktiviert SSL 3.0 auf Betriebssystemebene. Ist SSL 3.0 bereits in der Registrierung explizit aktiviert oder deaktiviert, wird diese Option nicht angezeigt und das Installationsprogramm führt keine Aktion aus. Wird die Option deaktiviert, führt das Installationsprogramm ebenfalls keine Aktion aus.
- 6 Folgen Sie den Anweisungen und schließen Sie die Installation ab.

Unbeaufsichtigte Installation des Plug-Ins „View Agent Direct-Connection“

Sie können die Microsoft Windows Installer-Funktion (MSI) für die unbeaufsichtigte Installation dazu verwenden, um das Plug-In „View Agent Direct-Connection“ zu installieren. Bei einer unbeaufsichtigten Installation verwenden Sie die Befehlszeile und müssen nicht auf Eingabeaufforderungen des Assistenten reagieren.

Die unbeaufsichtigte Installation ermöglicht eine effiziente Bereitstellung des VADC-Plug-Ins in einem großen Unternehmen. Weitere Informationen zum Windows Installer finden Sie unter „Befehlszeilenoptionen für Microsoft Windows Installer“ im Dokument *Einrichten von virtuellen Desktops in Horizon 7*. Das VADC-Plug-In unterstützt die folgenden MSI-Eigenschaften.

Tabelle 1-1. MSI-Eigenschaften für die unbeaufsichtigte Installation des Plug-Ins „View Agent Direct-Connection“

MSI-Eigenschaft	Beschreibung	Standardwert
LISTENPORT	Der TCP-Port, den das VADC-Plug-In verwendet, um Remote-Verbindungen zu akzeptieren. Standardmäßig konfiguriert das Installationsprogramm die Windows-Firewall so, dass der Verkehr im Port zugelassen wird.	443
MODIFYFIREWALL	Wenn 1 festgelegt ist, konfiguriert das Installationsprogramm die Windows-Firewall so, dass der Verkehr auf LISTENPORT zugelassen wird. Wenn 0 festgelegt ist, führt das Installationsprogramm dies nicht durch.	1
DISABLE_SSLV3	Ist SSL 3.0 in der Registrierung bereits explizit aktiviert oder deaktiviert, ignoriert das Installationsprogramm diese Eigenschaft. Andernfalls deaktiviert das Installationsprogramm SSL 3.0 auf Betriebssystemebene, wenn diese Eigenschaft auf „1“ festgelegt ist bzw. führt keine Aktion aus, wenn die Eigenschaft auf „0“ festgelegt ist.	1

Voraussetzungen

- Stellen Sie sicher, dass Horizon Agent installiert ist. Wenn in Ihrer Umgebung der Horizon-Verbindungsserver nicht vorhanden ist, installieren Sie Horizon Agent über die Befehlszeile und legen Sie einen Parameter fest, der Horizon Agent veranlasst, sich nicht beim Horizon-Verbindungsserver zu registrieren. Siehe [Installieren von Horizon 7 Agent für HTML Access](#).

Verfahren

- 1 Öffnen Sie eine Windows-Eingabeaufforderung.
- 2 Führen Sie die Installationsdatei für das VADC-Plug-In mit den Befehlszeilenoptionen aus, um eine unbeaufsichtigte Installation anzugeben. Optional können Sie zusätzliche MSI-Eigenschaften angeben.

Im folgenden Beispiel wird das VADC-Plug-In mit Standardoptionen installiert.

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

Im folgenden Beispiel wird das VADC-Plug-In installiert und ein TCP-Port angegeben, den VADC für Remote-Verbindungen abhören wird.

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

Erweiterte Konfiguration des Plug-Ins „View Agent Direct-Connection“

2

Sie können die standardmäßigen Konfigurationseinstellungen des Plug-Ins „View Agent Direct-Connection“ verwenden oder sie über Windows Active Directory-Gruppenrichtlinienobjekte (GPOs) anpassen bzw. sie über bestimmte Windows-Registrierungseinstellungen ändern.

Dieses Kapitel enthält die folgenden Themen:

- [Konfigurationseinstellungen des Plug-Ins „View Agent Direct-Connection“](#)
- [Deaktivieren von schwachen Verschlüsselungen in SSL/TLS](#)
- [Ersetzen des standardmäßigen selbstsignierten TLS-Serverzertifikats](#)
- [Autorisierung von Horizon Client für den Zugriff auf Desktops und Anwendungen](#)
- [Verwenden der Netzwerkadressübersetzung \(NAT\) und Portzuordnung](#)
- [Hinzufügen einer Zertifizierungsstelle zum Windows-Zertifikatspeicher](#)

Konfigurationseinstellungen des Plug-Ins „View Agent Direct-Connection“

Die ADMX-Vorlagendatei (`view_agent_direct_connection.admx`) für die VMware View Agent-Konfiguration enthält Richtlinieneinstellungen in Bezug auf die Authentifizierung und das View Agent Direct-Connection-Plug-In.

Die Konfigurationseinstellungen für View Agent Direct-Connection befinden sich im Gruppenrichtlinienverwaltungs-Editor unter **Computerkonfiguration > Administrative Vorlagen > VMware View Agent-Konfiguration > Konfiguration von View Agent Direct-Connection**.

Tabelle 2-1. Konfigurationseinstellungen des Plug-Ins „View Agent Direct-Connection“

Einstellung	Beschreibung
Anwendungen aktiviert	Diese Einstellung unterstützt den Anwendungsstart auf Remotedesktop-Sitzungshosts. Die Standardeinstellung ist aktiviert.
Wertepaare für Clientkonfigurationsname	Liste der Werte, die an den Client übergeben werden sollen, im Format Name=Wert. Beispiel: <code>clientCredentialCacheTimeout=1440</code> .
Zeitüberschreitung bei der Zwischenspeicherung der Client-Anmeldeinformationen	Der Zeitraum in Minuten, in dem ein Horizon Client einem Benutzer erlaubt, ein gespeichertes Kennwort zu verwenden. 0 bedeutet nie, -1 bedeutet immer. Horizon Client bietet Benutzern die Option, ihre Kennwörter zu speichern, wenn diese Einstellung auf einen gültigen Wert festgelegt ist. Der Standardwert lautet 0 (nie).

Tabelle 2-1. Konfigurationseinstellungen des Plug-Ins „View Agent Direct-Connection“ (Fortsetzung)

Einstellung	Beschreibung
Zeitüberschreitung der Clientsitzung	Die maximale Zeitdauer in Sekunden, in der eine Sitzung aktiv bleibt, wenn kein Client verbunden ist. Der Standardwert beträgt 36000 Sekunden (10 Stunden).
Client-Einstellung: AlwaysConnect	Der Wert kann auf TRUE oder FALSE festgelegt werden. Die Einstellung „AlwaysConnect“ wird an Horizon Client gesendet. Wenn diese Richtlinie auf TRUE festgelegt wird, werden alle gespeicherten Client-Voreinstellungen überschrieben. Standardmäßig wird kein Wert festgelegt. Durch das Aktivieren dieser Richtlinie wird der Wert auf TRUE festgelegt. Durch das Deaktivieren dieser Richtlinie wird der Wert auf FALSE festgelegt.
Clienteinstellung: AutoConnect	Diese Einstellung setzt alle gespeicherten Horizon Client-Voreinstellungen außer Kraft. Standardmäßig wird kein Wert festgelegt. Durch Aktivierung dieser Richtlinie wird der Wert auf „True“ festgelegt, eine Deaktivierung setzt den Wert auf „False“.
Clienteinstellung: ScreenSize	Legt die Einstellung für ScreenSize (Bildschirmgröße) fest, die an Horizon Client gesendet wird. Wenn dies aktiviert ist, werden alle gespeicherten Clientvoreinstellungen außer Kraft gesetzt. Falls dies deaktiviert oder nicht konfiguriert ist, werden die Clientvoreinstellungen verwendet.
Standardprotokoll	Das Standardanzeigeprotokoll, das von Horizon Client für die Herstellung einer Verbindung mit dem Desktop verwendet wird. Wenn hierfür kein Wert festgelegt ist, wird als Standardwert BLAST verwendet.
Haftungsausschluss aktiviert	Der Wert kann auf TRUE oder FALSE festgelegt werden. Wenn diese Einstellung auf TRUE gesetzt wird, zeigen Sie den Text des Haftungsausschlusses für die Benutzerakzeptanz bei der Anmeldung an. Der Text aus „Text des Haftungsausschlusses“ oder aus dem Gruppenrichtlinienobjekt Konfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Sicherheitsoptionen: Interaktive Anmeldung wird angezeigt. Die Standardeinstellung für „disclaimerEnabled“ ist FALSE.
Text des Haftungsausschlusses	Der den Benutzern von Horizon Client bei der Anmeldung angezeigte Text des Haftungsausschlusses. Die Richtlinie „Haftungsausschluss aktiviert“ muss auf TRUE festgelegt werden. Wenn der Text nicht festgelegt wird, wird standardmäßig der Wert über die Windows-Richtlinie Configuration\Windows Settings\Security Settings\Local Policies\Security Options verwendet.
Externer Blast-Port	Die Portnummer, die an Horizon Client für die TCP-Portnummer des Ziels gesendet wird, die für das HTML5/Blast-Protokoll verwendet wird. Ein Pluszeichen vor der Zahl gibt eine relative Zahl aus der für HTTPS verwendeten Portnummer an. Legen Sie diesen Wert nur fest, wenn die extern angezeigte Portnummer nicht mit dem Port übereinstimmt, den der Dienst verwaltet. Diese Portnummer befindet sich in der Regel in einer NAT-Umgebung. Standardmäßig wird kein Wert festgelegt.
Externer Framework-Kanal-Port	Die Portnummer, die an Horizon Client für die TCP-Portnummer des Ziels gesendet wird, die für das Framework-Kanal-Protokoll verwendet wird. Ein Pluszeichen vor der Zahl gibt eine relative Zahl aus der für HTTPS verwendeten Portnummer an. Legen Sie diesen Wert nur fest, wenn die extern angezeigte Portnummer nicht mit dem Port übereinstimmt, im dem der Dienst verwaltet. Diese Portnummer befindet sich in der Regel in einer NAT-Umgebung. Standardmäßig wird kein Wert festgelegt.
Externe IP-Adresse	Die IPV4-Adresse, die an Horizon Client für die IP-Adresse des Ziels gesendet wird, die für sekundäre Protokolle (RDP, PCoIP, Framework-Kanal usw.) verwendet wird. Legen Sie diesen Wert nur fest, wenn die extern angezeigte Adresse nicht mit der Adresse des Desktop-Computers übereinstimmt. Diese Adresse befindet sich in der Regel in einer NAT-Umgebung. Standardmäßig wird kein Wert festgelegt.

Tabelle 2-1. Konfigurationseinstellungen des Plug-Ins „View Agent Direct-Connection“ (Fortsetzung)

Einstellung	Beschreibung
Externer PCoIP-Port	Die Portnummer, die an Horizon Client für die TCP/UDP-Portnummer des Ziels gesendet wird, die für das PCoIP-Protokoll verwendet wird. Ein Pluszeichen vor der Zahl gibt eine relative Zahl aus der für HTTPS verwendeten Portnummer an. Legen Sie diesen Wert nur fest, wenn die extern angezeigte Portnummer nicht mit dem Port übereinstimmt, den der Dienst verwaltet. Diese Portnummer befindet sich in der Regel in einer NAT-Umgebung. Standardmäßig wird kein Wert festgelegt.
Externer RDP-Port	Die Portnummer, die an Horizon Client für die TCP-Portnummer des Ziels gesendet wird, die für das RDP-Protokoll verwendet wird. Ein Pluszeichen vor der Zahl gibt eine relative Zahl aus der für HTTPS verwendeten Portnummer an. Legen Sie diesen Wert nur fest, wenn die extern angezeigte Portnummer nicht mit dem Port übereinstimmt, den der Dienst verwaltet. Diese Portnummer befindet sich in der Regel in einer NAT-Umgebung. Standardmäßig wird kein Wert festgelegt.
HTTPS-Portnummer	Der TCP-Port, an dem das Plug-In eingehende HTTPS-Anforderungen von Horizon Client überwacht. Wenn dieser Wert geändert wird, müssen Sie eine entsprechende Änderung an der Windows-Firewall vornehmen, um eingehenden Datenverkehr zuzulassen. Die Standardeinstellung ist 443.
Multimedia-Umleitung (MMR) aktiviert	<p>Legt fest, ob MMR für Clientsysteme aktiviert ist. MMR ist ein Microsoft DirectShow-Filter, der Multimediadaten von bestimmten Codecs auf Horizon-Desktops direkt über einen TCP-Socket an das Clientsystem weiterleitet. Die Daten werden direkt auf dem Clientsystem decodiert, auf dem sie wiedergegeben werden. Standardmäßig ist diese Richtlinie deaktiviert.</p> <p>MMR arbeitet nicht ordnungsgemäß, wenn die Hardware zur Videoanzeige auf dem Clientsystem keine Overlay-Unterstützung bietet. Clientsysteme verfügen eventuell nicht über ausreichend Ressourcen zur Verarbeitung der lokalen Multimedia-Decodierung.</p>
Zurücksetzen aktiviert	Der Wert kann auf TRUE oder FALSE festgelegt werden. Wenn diese Einstellung auf TRUE gesetzt wird, kann ein authentifizierter Horizon Client einen Neustart auf Betriebssystemebene durchführen. Diese Einstellung ist standardmäßig deaktiviert (FALSE).
Zeitüberschreitung der Sitzung	Der Zeitraum, in dem ein Benutzer eine Sitzung geöffnet lassen kann, nachdem er sich über Horizon Client angemeldet hat. Der Wert wird in Minuten festgelegt. Der Standardwert lautet 600 Minuten. Wenn die Zeitüberschreitung erreicht wurde, werden alle Desktop- und Anwendungssitzungen eines Benutzers getrennt.
USB-AutoConnect	Der Wert kann auf TRUE oder FALSE festgelegt werden. Verbinden Sie USB-Geräte mit dem Desktop, wenn sie angeschlossen sind. Wenn diese Richtlinie festgelegt ist, wird sie von allen gespeicherten Client-Voreinstellungen überschrieben. Standardmäßig wird kein Wert festgelegt.
USB aktiviert	Der Wert kann auf TRUE oder FALSE festgelegt werden. Legt fest, ob Desktops USB-Geräte verwenden können, die mit dem Clientsystem verbunden sind. Der Standardwert ist aktiviert. Um aus Sicherheitsgründen die Verwendung externer Geräte zu unterbinden, deaktivieren Sie die Einstellung (FALSE).
Zeitüberschreitung des Benutzerleerlaufs	Wenn auf dem Horizon Client für diesen Zeitraum keine Benutzeraktivität vorhanden ist, werden die Desktop- und Anwendungssitzungen des Benutzers getrennt. Der Wert wird in Sekunden festgelegt. Der Standardwert beträgt 900 Sekunden (15 Minuten).

Tabelle 2-1. Konfigurationseinstellungen des Plug-Ins „View Agent Direct-Connection“ (Fortsetzung)

Einstellung	Beschreibung
X509-Zertifikatauthentifizierung	Legt fest, ob die Zertifikatauthentifizierung mit Smartcard X.509 deaktiviert, zulässig oder erforderlich ist.
X509-SSL-Zertifikatauthentifizierung aktiviert	Legt fest, ob die Zertifikatauthentifizierung mit Smartcard X.509 über eine direkte SSL-Verbindung von einem Horizon Client aktiviert wird. Diese Option ist nicht erforderlich, wenn die X.509-Zertifikatauthentifizierung über einen zwischenzeitlichen SSL-Beendigungspunkt durchgeführt wird. Wenn Sie diese Einstellung ändern, muss Horizon Agent neu gestartet werden.

Die Werte „Externe Portnummer“ und „Externe IP-Adresse“ werden für die Unterstützung der Netzwerkadressübersetzung (NAT) und Portzuordnung verwendet. Weitere Informationen finden Sie unter [Verwenden der Netzwerkadressübersetzung \(NAT\) und Portzuordnung](#).

Für die Smartcard-Authentifizierung muss sich die Zertifizierungsstelle (CA), die die Smartcard-Zertifikate signiert, im Windows-Zertifikatspeicher befinden. Informationen zum Hinzufügen einer Zertifizierungsstelle finden Sie unter [Hinzufügen einer Zertifizierungsstelle zum Windows-Zertifikatspeicher](#).

Hinweis Wenn ein Benutzer versucht, sich mit einer Smartcard bei einem Computer mit Windows 7 oder Windows Server 2008 R2 anzumelden, und das Smartcard-Zertifikat wurde durch eine Zwischen-Zertifizierungsstelle unterzeichnet, schlägt der Versuch möglicherweise fehl, da Windows an den Client eine Liste der vertrauenswürdigen Aussteller senden kann, die keine Zwischen-Zertifizierungsstellennamen enthält. In diesem Fall kann der Client kein entsprechendes Smartcard-Zertifikat auswählen. Zur Vermeidung dieses Problems legen Sie den Registrierungswert SendTrustedIssuerList (REG_DWORD) im Registrierungsschlüssel HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL auf „0“ fest. Wenn dieser Registrierungswert auf „0“ festgelegt ist, sendet Windows keine Liste mit vertrauenswürdigen Ausstellern an den Client, der dann alle gültigen Zertifikate für die Smartcard auswählen kann.

Deaktivieren von schwachen Verschlüsselungen in SSL/TLS

Zur Erhöhung der Sicherheit können Sie das Domänenrichtlinien-GPO (Gruppenrichtlinienobjekt) konfigurieren und sicherstellen, dass eine Kommunikation, die das SSL/TLS-Protokoll zwischen Horizon Client und auf virtuellen Maschinen basierenden Desktops oder RDS-Hosts verwendet, keine schwachen Verschlüsselungen zulässt.

Verfahren

- 1 Bearbeiten Sie auf dem Active Directory-Server das GPO, indem Sie **Start > Verwaltung > Gruppenrichtlinienverwaltung** wählen, mit der rechten Maustaste auf das GPO klicken und **Bearbeiten** auswählen.
- 2 Im Editor der Gruppenrichtlinienverwaltung wechseln Sie zu **Computerkonfiguration > Richtlinien > Administratorvorlagen > Netzwerk > SSL-Konfigurationseinstellungen**.

- 3 Doppelklicken Sie auf **Reihenfolge der SSL-Verschlüsselungssammlungen**.
- 4 Im Fenster „Reihenfolge der SSL-Verschlüsselungssammlungen“ klicken Sie auf **Aktiviert**.
- 5 Im Bereich „Optionen“ ersetzen Sie den gesamten Inhalt des Textfeldes „SSL-Verschlüsselungssammlungen“ mit der folgenden Verschlüsselungsliste:

```
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
```

Die Verschlüsselungssammlungen sind oben in gesonderten Zeilen zur besseren Lesbarkeit aufgeführt. Wenn Sie die Liste in das Textfeld einfügen, müssen die Verschlüsselungssammlungen in einer Zeile ohne Leerzeichen nach den einzelnen Trennkommas enthalten sein.

- 6 Beenden Sie den Editor der Gruppenrichtlinienverwaltung.
- 7 Starten Sie die VADC-Maschinen neu, damit die neue Gruppenrichtlinie übernommen wird.

Hinweis Wenn Horizon Client nicht für die Unterstützung einer Verschlüsselung konfiguriert ist, die vom virtuellen Desktop-Betriebssystem unterstützt wird, schlägt die TLS/SSL-Aushandlung fehl und der Client kann keine Verbindung herstellen.

Weitere Informationen zur Konfiguration von unterstützten Verschlüsselungssammlungen in Horizon Clients finden Sie in der Dokumentation Horizon Client unter https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

Ersetzen des standardmäßigen selbstsignierten TLS-Serverzertifikats

Ein selbstsigniertes TLS-Serverzertifikat kann Horizon Client keinen ausreichenden Schutz vor Bedrohungen durch Sabotage und Überwachung bieten. Um Ihre Desktops vor diesen Bedrohungen zu schützen, müssen Sie das erzeugte selbstsignierte Zertifikat ersetzen.

Wenn das VADC-Plug-In (View Agent Direct-Connection) zum ersten Mal nach der Installation startet, erzeugt es automatisch ein selbstsigniertes TLS-Serverzertifikat und platziert es im Windows-Zertifikatspeicher. Das TLS-Serverzertifikat wird Horizon Client während der TLS-Protokoll-Aushandlung vorgelegt, um Informationen zum Client über diesen Desktop bereitzustellen. Dieses standardmäßige selbstsignierte TLS-Serverzertifikat kann keine Garantien über diesen Desktop bieten, es sei denn, es wird durch ein von einer Zertifizierungsstelle signiertes Zertifikat ersetzt. Diese Stelle muss vom Client als vertrauenswürdig eingestuft und durch die Zertifikatprüfungen von Horizon Client validiert sein.

Die Vorgehensweise für die Speicherung dieses Zertifikats im Windows-Zertifikatspeicher und die Vorgehensweise zum Ersetzen durch ein angemessenes, von einer Zertifizierungsstelle signiertes Zertifikat sind identisch mit denen, die für den Horizon 7-Verbindungsserver verwendet werden. Informationen zur Vorgehensweise für das Ersetzen des Zertifikats finden Sie unter „Konfigurieren von TLS-Zertifikaten für Horizon 7-Server“ im Dokument *Horizon 7-Installation*.

Zertifikate mit SAN (Subject Alternative Name) und Platzhalterzertifikate werden unterstützt.

Hinweis Um die von einer Zertifizierungsstelle signierten TLS-Serverzertifikate mithilfe des View Agent Direct-Connection-Plug-Ins auf einer großen Anzahl von Desktops zu verteilen, verwenden Sie die Active Directory-Registrierung, um die Zertifikate an jede virtuelle Maschine zu verteilen. Weitere Informationen finden Sie unter <http://technet.microsoft.com/en-us/library/cc732625.aspx>.

Autorisierung von Horizon Client für den Zugriff auf Desktops und Anwendungen

Der Autorisierungsmechanismus, der einem Benutzer den direkten Zugriff auf Desktops und Anwendungen ermöglicht, wird in der lokalen Betriebssystemgruppe **View Agent Direct-Connection-Benutzer** gesteuert.

Wenn ein Benutzer Mitglied dieser Gruppe ist, ist der Benutzer berechtigt, eine Verbindung zum VM-basierten Desktop, zum veröffentlichten Desktop oder zu den veröffentlichten Anwendungen herzustellen. Wenn das Plug-In erstmalig installiert wird, wird die lokale Gruppe erstellt und diese enthält die Gruppe „Authentifizierte Benutzer“. Jeder, der vom Plug-In erfolgreich authentifiziert wird, ist berechtigt, auf den Desktop oder die Anwendungen zuzugreifen.

Um den Zugriff auf diesen Desktop oder den RDS-Host einzuschränken, können Sie die Mitgliedschaft dieser Gruppe ändern, um eine Liste von Benutzern und Benutzergruppen festzulegen. Bei den Benutzern kann es sich um lokale oder Domänenbenutzer und Benutzergruppen handeln. Wenn sich der Benutzer nicht in dieser Gruppe befindet, erhält der Benutzer nach der Authentifizierung eine Nachricht mit der Information, dass der Benutzer nicht berechtigt ist, auf den VM-basierten Desktop bzw. den veröffentlichten Desktop und auf Anwendungen zuzugreifen, die auf diesem RDS-Host gehostet werden.

Verwenden der Netzwerkadressübersetzung (NAT) und Portzuordnung

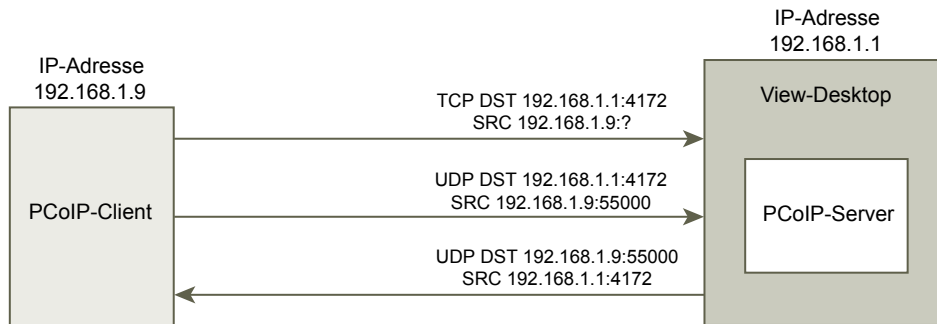
Die Netzwerkadressübersetzung (NAT) und Portzuordnungskonfiguration sind erforderlich, wenn Horizon Clients eine Verbindung zu VM-basierten Desktops auf verschiedenen Netzwerken herstellt.

In den hier enthaltenen Beispielen müssen Sie die externen Adressierungsinformationen auf dem Desktop konfigurieren, sodass Horizon Client diese Informationen zum Herstellen einer Verbindung zum Desktop verwenden kann, indem NAT oder ein Portzuordnungs-Gerät verwendet wird. Dieser URL ist mit den Einstellungen „Externer URL“ und „PCoIP -Externer URL“ auf dem Horizon 7-Verbindungsserver und -Sicherheitsserver identisch.

Wenn Horizon Client sich auf einem anderen Netzwerk befindet, ein NAT-Gerät sich zwischen Horizon Client befindet und das Desktop das Plug-In ausführt, ist eine NAT- oder Portzuordnungskonfiguration erforderlich. Beispiel: Wenn sich eine Firewall zwischen dem Horizon Client und dem Desktop befindet, fungiert die Firewall als NAT- bzw. Portzuordnungsgerät.

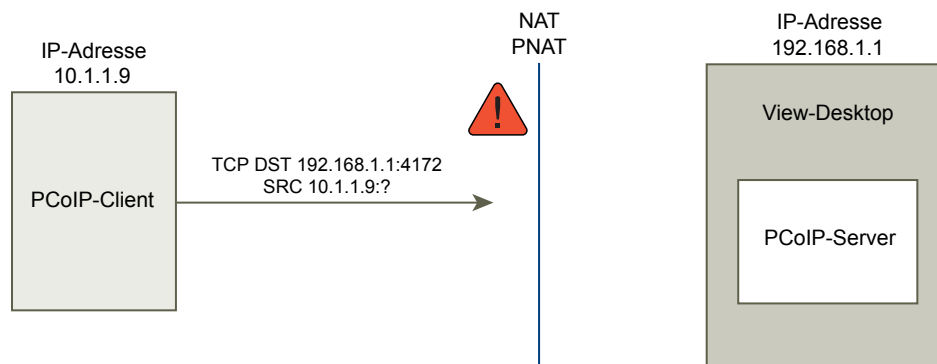
Eine Beispiel-Bereitstellung eines Desktops mit der IP-Adresse 192.168.1.1 veranschaulicht die Konfiguration der NAT und Portzuordnung. Ein Horizon Client-System mit einer IP-Adresse von 192.168.1.9 auf demselben Netzwerk stellt durch die Verwendung von TCP und UDP eine PCoIP-Verbindung her. Diese Verbindung wird als direkt ohne NAT- bzw. Portzuordnungskonfiguration bezeichnet.

Abbildung 2-1. Direkt-PCoIP aus einem Client auf demselben Netzwerk



Wenn Sie ein NAT-Gerät zwischen dem Client und dem Desktop hinzufügen, sodass sie in einem anderen Adressbereich betrieben werden, und keine Konfigurationsänderungen am Plug-In durchführen, werden die PCoIP-Pakete nicht ordnungsgemäß umgeleitet und schlagen fehl. In diesem Beispiel verwendet der Client einen anderen Adressbereich und hat die IP-Adresse 10.1.1.9. Dieses Setup schlägt fehl, da der Client die Adresse des Desktops verwenden wird, um die TCP- und UDP-PCoIP-Pakete zu senden. Die Zieladresse 192.168.1.1 funktioniert nicht über das Client-Netzwerk und kann dazu führen, dass der Client einen leeren Bildschirm anzeigt.

Abbildung 2-2. PCoIP aus einem Client über ein NAT-Gerät mit Fehler

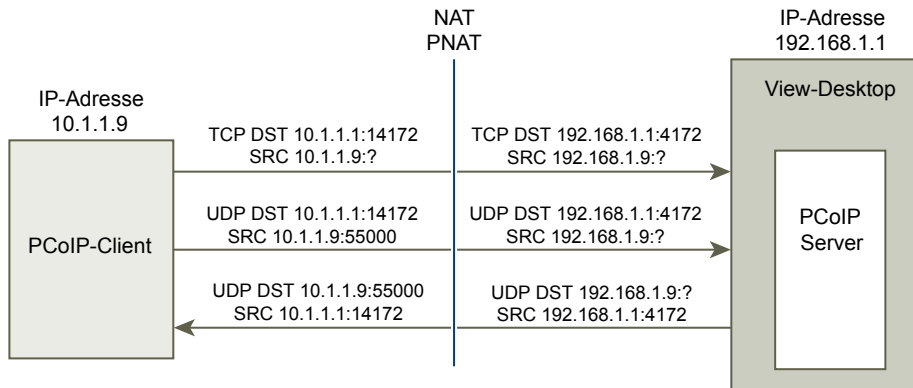


Um dieses Problem zu lösen, müssen Sie das Plug-In für die Verwendung einer externen IP-Adresse konfigurieren. Falls externalIPAddress für diesen Desktop als 10.1.1.1 konfiguriert ist, weist das Plug-In dem Client die IP-Adresse 10.1.1.1 zu, wenn Desktop-Protokollverbindungen zum Desktop hergestellt werden. Der Dienst „PCoIP Secure Gateway“ muss für PCoIP auf dem Desktop für dieses Setup gestartet werden.

Wenn der Desktop den standardmäßigen PCoIP-Port 4172 für die Portzuordnung verwendet, der Client jedoch einen anderen Zielport verwenden muss, welcher zum Port 4172 auf dem Portzuordnungsgerät zugewiesen ist, müssen Sie das Plug-In für dieses Setup konfigurieren. Wenn das Portzuordnungsgerät den Port 14172 zu 4172 zuordnet, muss der Client einen Zielport von 14172 für PCoIP verwenden. Sie müssen dieses Setup für PCoIP konfigurieren. Legen Sie `externalPCoIPPort` im Plug-In auf 14172 fest.

In einer Konfiguration, die NAT und Portzuordnung verwendet, ist `externalIPAddress` auf 10.1.1.1 festgelegt, das über das Netzwerk in 192.168.1.1 übertragen wird. Außerdem wird `externalPCoIPPort` auf 14172 festgelegt, das über den Port zu 4172 zugewiesen ist.

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



Sie müssen `externalRDPPort` und `externalFrameworkChannelPort` konfigurieren, um die TCP-Portnummer anzugeben, die der Client zum Herstellen der Verbindungen über ein Portzuweisungsgerät verwendet – wie bei der externen PCoIP-TCP/UDP-Portkonfiguration für PCoIP, wenn der RDP-Port (3389) bzw. der Framework-Kanal-Port (32111) über den Port zugewiesen ist.

Erweitertes Adressierungsschema

Wenn Sie VM-basierte Desktops für den Zugriff über ein NAT- und Portzuweisungsgerät auf derselben externen IP-Adresse konfigurieren, müssen Sie jedem Desktop einen eindeutigen Satz Portnummern geben. Die Clients können dann dieselbe Ziel-IP-Adresse verwenden, verwenden aber eine eindeutige TCP-Portnummer für die HTTPS-Verbindung, um die Verbindung auf einen bestimmten virtuellen Desktop umzuleiten.

Beispielsweise leitet HTTPS-Port 1000 zu einem Desktop und HTTPS-Port 1005 zu einem anderen um, wobei beide dieselbe Ziel-IP-Adresse verwenden. In diesem Fall wäre die Konfiguration von eindeutigen externen Portnummern für jeden Desktop für die Desktop-Protokollverbindungen zu komplex. Aus diesem Grund können die Plug-In-Einstellungen `externalPCoIPPort`, `externalRDPPort` und `externalFrameworkChannelPort` einen optionalen relationalen Ausdruck annehmen anstatt eines statischen Werts, um eine Portnummer zu definieren, die relativ zur Grund-HTTPS-Portnummer ist, die vom Client verwendet wird.

Falls das Portzuweisungsgerät Portnummer 1000 für HTTPS mit einer Zuweisung zu TCP 443, Portnummer 1001 für RDP mit einer Zuweisung zu TCP 3389, Portnummer 1002 für PCoIP mit einer Zuweisung zu TCP und UDP 4172 und Portnummer 1003 für den Framework-Kanal mit einer Zuweisung zu TCP 32111 zur Vereinfachung der Konfiguration verwendet, können die externen Portnummern so konfiguriert

werden, dass `externalRDPport=+1`, `externalPCoIPport=+2` und `externalFrameworkChannelPort=+3` ist. Wenn die HTTPS-Verbindung von einem Client hereinkommt, der die HTTPS-Ziel-Portnummer 1000 verwendet hat, würden die externen Portnummern automatisch relativ zu dieser Portnummer 1000 berechnet und würden 1001, 1002 bzw. 1003 verwenden.

Um einen anderen virtuellen Desktop bereitzustellen, wenn das Portzuweisungsgerät Portnummer 1005 für HTTPS mit Zuweisung zu TCP 443, Portnummer 1006 für RDP mit Zuweisung zu TCP 3389, Portnummer 1007 für PCoIP mit Zuweisung zu TCP und UDP 4172 und Portnummer 1008 für den Framework-Kanal mit Zuweisung zu TCP 32111 verwendet, wobei genau dieselbe externe Portkonfiguration auf dem Desktop verwendet wird (+1, +2, +3 usw.), wenn die HTTPS-Verbindung von einem Client hereinkommt, würden die externen Portnummern automatisch relativ zu dieser Portnummer 1005 berechnet und würden 1006, 1007 bzw. 1008 verwenden.

Dieses Schema ermöglicht, dass alle Desktops identisch konfiguriert werden und doch dieselbe externe IP-Adresse nutzen. Durch die Zuteilung von Portnummern in Fünfer-Sprüngen (1000, 1005, 1010 ...) für die Basis-HTTPS-Portnummer wäre es möglich, auf über 12.000 virtuelle Desktops auf derselben IP-Adresse zuzugreifen. Basierend auf der Konfiguration des Portzuweisungsgeräts wird die Basis-Portnummer verwendet, um den virtuellen Desktop festzulegen, auf den die Verbindung geleitet werden soll. Wenn auf allen virtuellen Desktops `externalIPAddress=10.20.30.40`, `externalRDPport=+1`, `externalPCoIPport=+2` und `externalFrameworkChannelPort=+3` konfiguriert ist, würde die Zuweisung zu virtuellen Desktops wie in der NAT- und Portzuweisungstabelle beschrieben erfolgen.

Tabelle 2-2. NAT- und Portzuweisungswerte

VM-Nr.	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

In diesen Beispiel stellt Horizon Client eine Verbindung zur IP-Adresse 10.20.30.40 und einer HTTPS-Zielporntnummer von $(1000 + n \times 5)$ her, wobei n die Desktopnummer ist. Um eine Verbindung zu Desktop 3 herzustellen, würde sich der Client mit 10.20.30.40:1015 verbinden. Dieses Adressschema vereinfacht das Konfigurationssetup für jeden Desktop erheblich. Alle Desktops werden mit identischer externer Adresse und Portkonfiguration konfiguriert. Die NAT- und Portzuweisungskonfiguration erfolgt innerhalb des NAT- und Portzuweisungsgeräts mit diesem konsistenten Muster, und alle Desktops können über eine einzige öffentliche IP-Adresse aufgerufen werden. Der Client würde typischerweise einen einzigen öffentlichen DNS-Namen verwenden, der auf diese IP-Adresse auflöst.

Hinzufügen einer Zertifizierungsstelle zum Windows-Zertifikatspeicher

Für die Smartcard-Authentifizierung muss sich die Zertifizierungsstelle (CA), die das Smartcard-Zertifikat signiert, im Windows-Zertifikatspeicher befinden. Andernfalls können Sie die Zertifizierungsstelle zum Windows-Zertifikatspeicher hinzufügen.

Voraussetzungen

Stellen Sie sicher, dass die Microsoft Management Console (MMC) das Zertifikat-Snap-In aufweist. Weitere Informationen finden Sie unter „Hinzufügen des Zertifikat-Snap-Ins zu MMC“ im Dokument *Horizon 7-Installation*.

Verfahren

- 1 Starten Sie MMC.
- 2 Erweitern Sie in der MMC-Konsole den Knoten **Zertifikate (Lokaler Computer)** und navigieren Sie zum Ordner **Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate**.

Wenn das Root-Zertifikat vorhanden ist und die Zertifikatskette keine Zwischenzertifikate enthält, beenden Sie MMC.
- 3 Klicken Sie mit der rechten Maustaste auf den Ordner **Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate** und klicken Sie auf **Alle Aufgaben > Importieren**.
- 4 Klicken Sie im **Zertifikatsimport-Assistenten** auf **Weiter** und navigieren Sie zum Speicherort des Stamm-Zertifizierungsstellenzertifikats.
- 5 Wählen Sie die Datei mit dem Stamm-Zertifizierungsstellenzertifikat aus und klicken Sie auf **Öffnen**.
- 6 Klicken Sie auf **Weiter**, klicken Sie auf **Weiter** und klicken Sie auf **Fertig stellen**.
- 7 Wenn das Smartcard-Zertifikat von einer Zwischenzertifizierungsstelle ausgestellt wird, importieren Sie alle Zwischenzertifikate in der Zertifikatskette.
 - a Navigieren Sie zum Ordner **Zertifikate (Lokaler Computer) > Zwischenzertifizierungsstellen > Zertifikate**.
 - b Wiederholen Sie die Schritte 3 bis 6 für jedes Zwischenzertifikat.

Einrichten von HTML Access

Das VADC-Plug-In (View Agent Direct-Connection) unterstützt HTML Access auf VM-basierten Desktops und veröffentlichten Desktops. HTML Access auf veröffentlichten Anwendungen wird nicht unterstützt.

Dieses Kapitel enthält die folgenden Themen:

- [Installieren von Horizon 7 Agent für HTML Access](#)
- [Einrichten der statischen Inhaltsübermittlung](#)
- [Einrichten eines von einer vertrauenswürdigen Zertifizierungsstelle signierten TLS-Serverzertifikats](#)
- [Deaktivieren des HTTP/2-Protokolls auf Windows 10- und Windows 2016-Desktops](#)

Installieren von Horizon 7 Agent für HTML Access

Um HTML Access zu unterstützen, müssen Sie Horizon 7 Agent auf dem VM-basierten Desktop mit einem bestimmten Parameter installieren.

Voraussetzungen

- Laden Sie die Horizon Agent-Installationsdatei von der VMware-Downloadseite unter <http://www.vmware.com/go/downloadview> herunter.

Der Dateiname des Installationsprogramms lautet `VMware-viewagent-y.y.y-xxxxxx.exe` für 32-Bit-Windows oder `VMware-viewagent-x86_64-y.y.y-xxxxxx.exe` für 64-Bit-Windows, wobei `y.y.y` die Versionsnummer und `xxxxxx` die Buildnummer ist.

Verfahren

- ◆ Installieren Sie Horizon 7 Agent über die Befehlszeile und legen Sie einen Parameter fest, der Horizon 7 veranlasst, sich nicht beim Horizon 7-Verbindungsserver zu registrieren.

In diesem Beispiel wird die 32-Bit-Version von Horizon 7 Agent installiert.

```
VMware-viewagent-y.y.y-xxxxxx.exe /v VDM_SKIP_BROKER_REGISTRATION=1
```

Nächste Schritte

Installieren Sie das Plug-In „View Agent Direct-Connection“. Siehe [Installieren des Plug-Ins „View Agent Direct-Connection“](#).

Einrichten der statischen Inhaltsübermittlung

Wenn der HTML Access-Client vom Desktop bedient werden muss, müssen Sie einige Setup-Aufgaben auf dem Desktop durchführen. Dadurch kann ein Benutzer in einem Desktop direkt auf einen Browser verweisen.

Voraussetzungen

- Laden Sie die `portal.war`-ZIP-Datei für Horizon HTML Access von der VMware-Downloadseite unter <http://www.vmware.com/go/downloadview> herunter.

Der Dateiname lautet `VMware-Horizon-View-HTML-Access-y.y.y-xxxxxx.zip`. Hierbei steht `y.y.y` für die Versionsnummer und `xxxxxx` für die Buildnummer.

Verfahren

- 1 Öffnen Sie die **Systemsteuerung**.
- 2 Wechseln Sie zu **Programme und Funktionen > Windows-Funktionen aktivieren oder deaktivieren**.
- 3 Aktivieren Sie das Kontrollkästchen **Internetinformationsdienste** und klicken Sie auf **OK**.
- 4 Wechseln Sie in der **Systemsteuerung** zu **Verwaltung > Internetinformationsdienste-Manager (IIS)**.
- 5 Erweitern Sie die Elemente im linken Fensterbereich
- 6 Klicken Sie mit der rechten Maustaste auf **Standardwebsite** und wählen Sie **Bindungen bearbeiten** aus.
- 7 Klicken Sie auf **Hinzufügen**.
- 8 Geben Sie **https**, **Keine zugewiesen** und den Port **443** an.
- 9 Wählen Sie im Feld **SSL-Zertifikat** das korrekte Zertifikat aus.

Option	Aktion
Das Zertifikat vdm ist vorhanden.	Wählen Sie vdm aus und klicken Sie auf OK .
Das Zertifikat vdm ist nicht vorhanden.	Wählen Sie vdmdefault aus und klicken Sie auf OK .

- 10 Entfernen Sie im Dialogfeld **Sitebindungen** den Eintrag für **HTTP-Port 80** und klicken Sie auf **Schließen**.
- 11 Klicken Sie auf **Standardwebsite**.
- 12 Doppelklicken Sie auf **MIME-Typen**.
- 13 Falls die **Dateierweiterung** „.json“ nicht vorhanden ist, klicken Sie im Bereich **Aktionen** auf **Hinzufügen....** Anderenfalls überspringen Sie die nächsten zwei Schritte.
- 14 Geben Sie für **Dateinamenerweiterung** **.json** ein.
- 15 Geben Sie für **MIME-Typ** den Wert **text/h323** ein und klicken Sie auf **OK**.

- 16 Geben Sie für **Dateinamenerweiterung** **.mem** ein.
- 17 Geben Sie für **MIME-Typ** den Wert **text/plain** ein und klicken Sie auf **OK**.
- 18 Kopieren Sie VMware-Horizon-View-HTML-Access-y.y.y-xxxxxx.zip in einen temporären Ordner.
- 19 Entzippen Sie die Datei VMware-Horizon-View-HTML-Access-y.y.y-xxxxxx.zip.
Das Ergebnis ist eine Datei mit dem Namen portal.war.
- 20 Benennen Sie portal.war in portal.zip um.
- 21 Entzippen Sie portal.zip in den Ordner C:\inetpub\wwwroot.
Passen Sie ggf. die Berechtigungen für den Ordner an, damit Dateien hinzugefügt werden können.
Der Ordner C:\inetpub\wwwroot\portal wird erstellt.
- 22 Öffnen Sie den **Editor**.
- 23 Erstellen Sie die Datei C:\inetpub\wwwroot\Default.htm mit dem folgenden Inhalt (ersetzen Sie *<IP-Adresse oder DNS-Name des Desktops>* durch die aktuelle IP-Adresse oder den aktuellen DNS-Namen des Desktops):

```
<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>
```

Einrichten eines von einer vertrauenswürdigen Zertifizierungsstelle signierten TLS-Serverzertifikats

Sie können ein von einer vertrauenswürdigen Zertifizierungsstelle signiertes TLS-Serverzertifikat einrichten, um sicherzustellen, dass es zwischen Clients und Desktops zu keinem missbräuchlichen Datenverkehr kommt.

Voraussetzungen

- Ersetzen Sie das standardmäßige selbstsignierte TLS-Serverzertifikat durch ein von einer vertrauenswürdigen Zertifizierungsstelle signiertes TLS-Serverzertifikat. Weitere Informationen finden Sie unter [Ersetzen des standardmäßigen selbstsignierten TLS-Serverzertifikats](#). Auf diese Weise wird ein Zertifikat erstellt, das als Wert für den Anzeigenamen **vdm** aufweist.

- Wenn die statischen Inhalte des Client über den Desktop bedient werden, richten Sie eine Bereitstellung von statischen Inhalten ein. Siehe [Einrichten der statischen Inhaltsübermittlung](#).
- Machen Sie sich mit dem Windows-Zertifikatspeicher vertraut. Weitere Informationen finden Sie unter „Konfigurieren des Verbindungsservers, Sicherheitsservers oder von View Composer für die Verwendung eines neuen TLS-Zertifikats“ im Dokument *Horizon 7-Installation*.

Verfahren

- 1 Navigieren Sie im Windows-Zertifikatspeicher zu **Persönlich > Zertifikate**.
- 2 Doppelklicken Sie auf das Zertifikat mit dem Anzeigenamen **vdm**.
- 3 Klicken Sie auf die Registerkarte **Details**.
- 4 Kopieren Sie den Wert **Thumbprint**.
- 5 Starten Sie den Windows-Registrierungs-Editor.
- 6 Navigieren Sie zum Registrierungsschlüssel HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config.
- 7 Fügen Sie einen neuen Zeichenfolgenwert (REG_SZ) SSLHash zu diesem Registrierungsschlüssel hinzu.
- 8 Setzen Sie den Wert SSLHash auf den Wert **Thumbprint**.

Deaktivieren des HTTP/2-Protokolls auf Windows 10- und Windows 2016-Desktops

Bei einigen Webbrowsern kann beim Zugriff auf einen Windows 10 VADC- oder einen Windows 2016 VADC-Desktop der Fehler ERR_SPDY_PROTOCOL_ERROR auftreten. Dieser Fehler lässt sich durch Deaktivierung des HTTP/2-Protokolls auf dem Desktop vermeiden.

Verfahren

- 1 Starten Sie den Windows-Registrierungs-Editor.
- 2 Wechseln Sie zum Registrierungsschlüssel HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\HTTP\Parameters.
- 3 Fügen Sie diesem Registrierungsschlüssel zwei neue REG_DWORD-Werte, EnableHttp2Tls und EnableHttp2Cleartext, hinzu.
- 4 Setzen Sie beide Werte auf **0**.
- 5 Starten Sie den Desktop neu.

Einrichten von VADC (View Agent Direct Connection) auf Remote-Desktop-Dienste-Hosts

4

Horizon 7 unterstützt RDS-Hosts (Remote Desktop Services), die veröffentlichte Desktops und Anwendungen bereitstellen, auf welche Benutzer über Horizon Clients zugreifen können. Ein veröffentlichter Desktop basiert auf einer Desktop-Sitzung zu einem RDS-Host. In einer typischen Horizon 7-Bereitstellung verbinden sich Clients mit Desktops und Anwendungen über den Horizon-Verbindungsserver. Wenn Sie jedoch das VADC-Plug-In (View Agent Direct-Connection) auf einem RDS-Host installieren, können sich Clients mit veröffentlichten Desktops oder Anwendungen verbinden, ohne den Horizon-Verbindungsserver zu verwenden.

Dieses Kapitel enthält die folgenden Themen:

- [RDS-Hosts](#)
- [Berechtigungen für veröffentlichte Desktops und Anwendungen](#)

RDS-Hosts

Ein RDS-Host (Remote Desktop Services) ist ein Servercomputer, der Anwendungen und Desktops für den Remotezugriff hostet.

In einer Horizon 7-Bereitstellung ist ein RDS-Host ein Windows-Server, der die Rolle Microsoft-Remote-Desktop-Dienste innehat, bei dem der Microsoft Remote-Desktop-Sitzungshost-Dienst aktiviert und Horizon Agent installiert ist. Ein RDS-Host kann View Agent Direct Connection (VADC) unterstützen, wenn auch das VADC-Plug-In installiert ist. Informationen zur Einrichtung eines RDS-Hosts und zur Installation von Horizon 7 Agent finden Sie unter „Einrichten von Remote-Desktop-Dienste-Hosts“ im Dokument *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*. Informationen zur Installation des VADC-Plug-Ins finden Sie unter [Kapitel 1 Installation des Plug-Ins „View Agent Direct-Connection“](#).

Hinweis Wenn Sie Horizon Agent installieren, fragt Sie das Installationsprogramm nach dem Hostnamen oder der IP-Adresse des Horizon-Verbindungservers, mit dem Horizon Agent eine Verbindung herstellen wird. Durch die Angabe eines Parameters bei der Installation können Sie dafür sorgen, dass das Installationsprogramm diesen Schritt überspringt.

```
VMware-viewagent-x86_64-y.y.y-xxxxxx.exe /v "VDM_SKIP_BROKER_REGISTRATION=1"
```

Nach der Einrichtung eines RDS-Hosts und der Installation des VADC-Plug-Ins müssen Sie Berechtigungen für RDS-Desktops und Anwendungen erteilen. Siehe [Berechtigungen für veröffentlichte Desktops und Anwendungen](#).

Berechtigungen für veröffentlichte Desktops und Anwendungen

Sie müssen den betreffenden Benutzern Berechtigungen für veröffentlichte Desktops und Anwendungen zuweisen, damit sie auf diese Desktops und Anwendungen zugreifen können.

Wenn auf dem RDS-Host Windows Server 2008 R2 SP1 ausgeführt wird, führen Sie **RemoteApp Manager** aus, um Berechtigungen zu konfigurieren.

Wenn auf dem RDS-Host Windows Server 2012 oder 2012 R2, ausgeführt wird, führen Sie **Server Manager** aus und navigieren Sie zu **Remote-Desktop-Dienste**, um Berechtigungen zu konfigurieren.

Desktop-Berechtigungen

Führen Sie die folgenden Schritte aus, um einen Benutzer zum Starten eines veröffentlichten Desktops zu berechtigen:

- Stellen Sie sicher, dass der betreffende Benutzer Mitglied der lokalen Gruppe **View Agent Direct-Connection-Benutzer** ist. Alle authentifizierten Benutzer sind standardmäßig Mitglieder dieser Gruppe.
- Stellen Sie unter Windows Server 2008 R2 SP1 in **RemoteApp Manager** sicher, dass der RD-Sitzungshostserver die Konfiguration **Remote-Desktop-Verbindung zu diesem RD-Sitzungshostserver unter 'RD-Webzugriff'** anzeigt aufweist.
- Führen Sie unter Windows 2012 oder 2012 R2 **Server Manager** aus und navigieren Sie zu **Remote-Desktop-Dienste**, um Berechtigungen zu konfigurieren.

Anwendungsberechtigungen

Führen Sie die folgenden Schritte aus, damit ein Benutzer eine Anwendung starten kann:

- Stellen Sie sicher, dass der betreffende Benutzer Mitglied der lokalen Gruppe **View Agent Direct-Connection-Benutzer** ist. Alle authentifizierten Benutzer sind standardmäßig Mitglieder dieser Gruppe.
- Stellen Sie unter Windows Server 2008 R2 SP1 in **RemoteApp Manager** sicher, dass die Anwendung unter **RemoteApp-Programme** aufgeführt ist, dass sie für **RD-Webzugriff** eingerichtet ist und dass für diese Anwendung Benutzerzuweisungen festgelegt sind, sei es für alle Benutzer, für diesen Benutzer oder für eine Gruppe, deren Mitglied der betreffende Benutzer ist.
- Führen Sie unter Windows 2012 oder 2012 R2 **Server Manager** aus und navigieren Sie zu **Remote-Desktop-Dienste**, um Berechtigungen zu konfigurieren.

Fehlerbehebung des Plug-Ins „View Agent Direct-Connection“

5

Bei der Verwendung des Plug-Ins „View Agent Direct-Connection“ treten möglicherweise bekannte Probleme auf.

Wenn Sie ein Problem mit dem Plug-In „View Agent Direct-Connection“ untersuchen, stellen Sie sicher, dass die richtige Version installiert ist und ausgeführt wird.

Wenn ein Problem durch den Support von VMware behoben werden soll, aktivieren Sie in einem solchen Fall immer die vollständige Protokollierung, reproduzieren Sie das Problem und generieren Sie einen DCT-Protokollsatz (Data Collection Tool). Der technische Support von VMware kann dann diese Protokolle analysieren. Details zur Erstellung eines DCT-Protokollsatzes finden Sie im VMware-Knowledgebase-Artikel „Sammeln von Diagnoseinformationen für VMware View“ unter <http://kb.vmware.com/kb/1017939>.

Dieses Kapitel enthält die folgenden Themen:

- [Falsche Grafikkarte wurde installiert](#)
- [Nicht genügend Video-RAM](#)
- [Aktivieren der vollständigen Protokollierung für das Einbeziehen von TRACE- und DEBUG-Informationen](#)

Falsche Grafikkarte wurde installiert

Damit PCoIP ordnungsgemäß funktioniert, muss die korrekte Version des Grafiktreibers installiert werden.

Problem

Wenn ein Benutzer mithilfe von PCoIP eine Verbindung zu einem Desktop oder einer Anwendung herstellt, wird ein schwarzer Bildschirm angezeigt.

Ursache

Eine falsche Version des Grafiktreibers wird ausgeführt. Dies kann geschehen, wenn nach der Installation von Horizon 7 Agent eine falsche Version von VMware Tools installiert wird.

Lösung

- ◆ Installieren Sie Horizon 7 Agent neu.

Nicht genügend Video-RAM

Um PCoIP-Unterstützung zu ermöglichen, muss eine virtuelle Maschine, auf der ein Desktop oder ein RDS-Host ausgeführt wird, über mindestens 128 MB an Video-RAM verfügen.

Problem

Wenn ein Benutzer mithilfe von PCoIP eine Verbindung zu einem Desktop oder einer Anwendung herstellt, wird ein schwarzer Bildschirm angezeigt.

Ursache

Die virtuelle Maschine verfügt nicht über genügend Video-RAM.

Lösung

- ◆ Konfigurieren Sie für jede virtuelle Maschine mindestens 128 MB an Video-RAM.

Aktivieren der vollständigen Protokollierung für das Einbeziehen von TRACE- und DEBUG-Informationen

Das View Agent Direct-Connection-Plug-In schreibt Protokolleinträge in das Standard-Horizon Agent-Protokoll. TRACE- und DEBUG-Informationen sind im Protokoll standardmäßig nicht enthalten.

Problem

Das Horizon 7 Agent-Protokoll enthält keine TRACE- und DEBUG-Informationen.

Ursache

Die vollständige Protokollierung ist nicht aktiviert. Sie müssen die vollständige Protokollierung aktivieren, um TRACE- und DEBUG-Informationen in das Horizon Agent-Protokoll aufzunehmen.

Lösung

- 1 Öffnen Sie eine Eingabeaufforderung und führen Sie `C:\Program Files\VMware\VMware View\Agent\DCT\support.bat loglevels` aus.
- 2 Geben Sie 3 für vollständige Protokollierung ein.

Die Debug-Protokolldateien befinden sich in `%ALLUSERSPROFILE%\VMware\VDM\logs`. Die Datei `debug*.log` enthält Informationen vom Horizon Agent und vom Plug-In. Suchen Sie nach `wsnm_xmlapi`, um die Plug-In-Protokollzeilen zu finden.

Wenn der Horizon Agent gestartet wird, 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, versi-
on=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
```