

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

VMware Horizon 6 6.0



vmware®

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

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

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

Copyright © 2019 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

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 selbst signierten SSL-Serverzertifikats	13
Autorisierung von Horizon Client für den Zugriff auf Desktops und Anwendungen	14
Verwenden der Netzwerkadressübersetzung (NAT) und Portzuordnung	14
Erweitertes Adressierungsschema	16
3 Einrichten von HTML Access	18
Installieren von View Agent für HTML Access	18
Einrichten der statischen Inhaltsübermittlung	19
Einrichten eines von einer vertrauenswürdigen Zertifizierungsstelle signierten SSL-Serverzertifikats	20
4 Einrichten von VADC (View Agent Direct Connection) auf Remote-Desktop-Dienste-Hosts	22
RDS-Hosts	22
Berechtigung für RDS-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“

Die *Verwaltung des Plug-Ins „View Agent Direct-Connection“* bietet Informationen über die Installation und Konfiguration des Plug-Ins „View Agent Direct-Connection“. Dieses Plug-In ist eine installierbare Erweiterung für View Agent, um einem Horizon Client ohne View-Verbindungsserver eine direkte Verbindung zu einem VM-basierten Desktop, einem Remote-Desktop-Dienste-Desktop oder einer Anwendung zu ermöglichen. Alle Desktop- und Anwendungsfunktionen funktionieren auf dieselbe Weise wie bei der Verbindung des Benutzers über den View-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 Datacenter-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, RDS-Desktops bzw. Anwendungen herzustellen. Das VADC-Plug-In ist eine Erweiterung von View 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 View Agent bereits installiert ist. Eine Liste der Betriebssysteme, die View Agent unterstützt, finden Sie unter „Unterstützte Betriebssysteme für View Agent“ im Dokument *Installation von View*.

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.
- Sie müssen VMware Tools installieren, bevor Sie View 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 View Agent installiert ist.

Verfahren

- 1 Laden Sie die Installationsdatei des VADC-Plug-Ins von der VMware-Produktseite unter <http://www.vmware.com/products/> 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 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 im Dokument *Einrichten von Desktop- und Anwendungspools in VMware Horizon View* unter „Befehlszeilenoptionen für Microsoft Windows Installer“. 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

Voraussetzungen

- Stellen Sie sicher, dass View Agent installiert ist.

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.

In diesem Beispiel wird das VADC-Plug-In mit Standardoptionen installiert.

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

In diesem 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 selbst signierten SSL-Serverzertifikats](#)
- [Autorisierung von Horizon Client für den Zugriff auf Desktops und Anwendungen](#)
- [Verwenden der Netzwerkadressübersetzung \(NAT\) und Portzuordnung](#)

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

Alle Konfigurationseinstellungen für das Plug-In „View Agent Direct-Connection“ werden in der lokalen Registrierung auf jedem VM-basierten Desktop oder RDS-Host gespeichert. Sie können diese Einstellungen unter Verwendung der Gruppenrichtlinienobjekte (GPOs) von Windows Active Directory über den lokalen Richtlinien-Editor oder durch das direkte Ändern der Registrierung verwalten.

Die Registrierungswerte befinden sich im Registrierungsschlüssel HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Agent\Configuration\XMLAPI.

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

Einstellung	Registrierungswert	Typ	Beschreibung
HTTPS-Portnummer	httpsPortNumber	REG_SZ	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.
Zeitüberschreitung der Sitzung	sessionTimeout	REG_SZ	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.
Haftungsausschluss aktiviert	disclaimerEnabled	REG_SZ	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 wird, wenn angegeben, über den „Text des Haftungsausschlusses“ angezeigt oder über das Gruppenrichtlinienobjekt Configuration\Windows Settings\Security Settings\Local Policies\Security Options: Interactive logon. Die Standardeinstellung für „disclaimerEnabled“ ist FALSE.
Text des Haftungsausschlusses	disclaimerText	REG_SZ	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.
Client-Einstellung: AlwaysConnect	alwaysConnect	REG_SZ	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.
Externer PCoIP-Port	externalPCoIPPort	REG_SZ	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.

Einstellung	Registrierungswert	Typ	Beschreibung
Externer Blast-Port	externalBlastPort	REG_SZ	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 RDP-Port	externalRDPPort	REG_SZ	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.
Externe IP-Adresse	externalIPAddress	REG_SZ	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.
Externer Framework-Kanal-Port	externalFrameworkChannelPort	REG_SZ	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.
USB aktiviert	usbEnabled	REG_SZ	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).
Client-Einstellung: USB-AutoConnect	usbAutoConnect	REG_SZ	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.

Einstellung	Registrierungswert	Typ	Beschreibung
Zurücksetzen aktiviert	resetEnabled	REG_SZ	Der Wert kann auf TRUE oder FALSE festgelegt werden. Wenn diese Einstellung auf TRUE gesetzt wird, kann ein authentifizierter Horizon Client einen Neustart der Ebene des Betriebssystems durchführen. Diese Einstellung ist standardmäßig deaktiviert (FALSE).
Zeitüberschreitung bei der Zwischenspeicherung der Client-Anmeldeinformationen	clientCredentialCacheTimeout	REG_SZ	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).
Zeitüberschreitung des Benutzerleerlaufs	userIdleTimeout	REG_SZ	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).

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](#).

Sie können Richtlinien festlegen, die diese Registrierungseinstellungen durch die Verwendung des lokalen Richtlinien-Editors oder der Gruppenrichtlinienobjekte in Active Directory überschreiben. Richtlinieneinstellungen haben Vorrang vor normalen Registrierungseinstellungen. Eine GPO-Vorlagendatei wird für die Konfiguration von Richtlinien bereitgestellt. Wenn View Agent und das Plug-In im standardmäßigen Speicherort installiert wurde, enthält die Vorlagendatei den folgenden Speicherort:

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

Sie können diese Vorlagendatei in Active Directory oder in den lokalen Gruppenrichtlinien-Editor importieren, um die Verwaltung dieser Konfigurationseinstellungen zu vereinfachen. Weitere Informationen zur Verwaltung der Richtlinieneinstellungen auf diese Weise finden Sie in der Dokumentation „Verarbeitung von Microsoft-Richtlinien-Editor und GPO“. Richtlinieneinstellungen für dieses Plug-In werden im Registrierungsschlüssel gespeichert:

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

Deaktivieren von schwachen Verschlüsselungen in SSL/TLS

Um eine größere Sicherheit zu erreichen, können Sie sicherstellen, dass die Kommunikation, die das SSL/TLS-Protokoll zwischen Horizon Clients und VM-basierten Desktops bzw. RDS-Hosts verwendet, schwache Verschlüsselungen nicht zulässt.

Die Konfiguration zum Deaktivieren von schwachen Verschlüsselungen wird in der Windows-Registrierung gespeichert. Änderungen an diesen Einstellungen müssen auf allen Computern vorgenommen werden, die das Plug-In „View Agent Direct-Connection“ ausführen.

Hinweis Diese Einstellungen wirken sich auf die sämtliche Nutzung von SSL/TLS auf dem Betriebssystem aus.

Sowohl SSL 3.0 als auch TLS 1.0 (RFC2246) mit INTERNET-DRAFT 56-bit Export Cipher Suites For TLS draft-ietf-tls-56-bit-ciphersuites-00.txt stellen Optionen für die Verwendung verschiedener Verschlüsselungssammlungen bereit. Jede Verschlüsselungssammlung bestimmt den Schlüsselaustausch, die Authentifizierung, die Verschlüsselung und die MAC-Algorithmen, die innerhalb einer SSL/TLS-Sitzung verwendet werden.

Voraussetzungen

Sie müssen über Erfahrung bei der Bearbeitung von Windows-Registrierungsschlüsseln verfügen, wenn Sie den Registrierungs-Editor Regedt32.exe verwenden.

Verfahren

- 1 Starten Sie den Registrierungs-Editor Regedt32.exe und suchen diesen Registrierungsschlüssel: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
- 2 Nehmen Sie Änderungen an der Registrierung vor.

Windows-Version	Registrierungsänderungen
XP SP3	<ul style="list-style-type: none"> ■ Fügen Sie im Unterschlüssel \Ciphers\DES_56/56 den DWORD-Wert Enabled mit dem Wert 0x0 hinzu. ■ Fügen Sie im Unterschlüssel \Hashes\MD5 den DWORD-Wert Enabled mit dem Wert 0x0 hinzu.
Vista und höher	<ul style="list-style-type: none"> ■ Erstellen Sie im Unterschlüssel \Hashes den Unterschlüssel MD5. ■ Fügen Sie im Unterschlüssel \Hashes\MD5 den DWORD-Wert Enabled mit dem Wert 0x0 hinzu.

- Die Registrierungsänderungen für Windows XP SP3 stellen sicher, dass nur die folgenden Verschlüsselungen verfügbar sind:
 - SSLv3 168 bits DES-CBC3-SHA
 - SSLv3 128 bits RC4-SHA
 - TLSv1 168 bits DES-CBC3-SHA
 - TLSv1 128 bits RC4-SHA
- Die Registrierungsänderungen für Windows Vista und höher stellen sicher, dass nur die folgenden Verschlüsselungen verfügbar sind:
 - SSLv3 168 Bit DES-CBC3-SHA
 - SSLv3 128 Bit RC4-SHA

- TLSv1 256 Bit AES256-SHA
- TLSv1 128 Bit AES128-SHA
- TLSv1 168 Bit DES-CBC3-SHA
- TLSv1 128 Bit RC4-SHA

Hinweis Beim Verbinden mit einem virtuellen Windows XP-Desktop über Horizon Client müssen Sie möglicherweise die Verschlüsselungsliste konfigurieren, die vom Client zum Einbeziehen einer Verschlüsselung über die unterstützte Liste auf Windows XP unterstützt wird. Beispiel: Möglicherweise müssen Sie den Client für die zusätzliche Unterstützung von TLSv1 128 Bits RC4-SHA konfigurieren. Standardmäßig unterstützt Horizon Client diese Verschlüsselung nicht mehr.

Wenn der 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 die Verbindung nicht 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 selbst signierten SSL-Serverzertifikats

Ein selbstsigniertes SSL-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 SSL-Server-Zertifikat und platziert es im Windows-Zertifikatspeicher. Das SSL-Server-Zertifikat wird Horizon Client während der SSL-Protokoll-Aushandlung vorgelegt, um Informationen zum Client über diesen Desktop bereitzustellen. Dieses standardmäßige selbstsignierte SSL-Server-Zertifikat kann keine Garantien über diesen Desktop bieten, es sei denn, es wird durch ein von einer Zertifizierungsstelle (CA) 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 CA-signiertes Zertifikat sind identisch mit denen, die für View-Verbindungsserver (Version 5.1 oder höher) verwendet werden. Details zur Vorgehensweise für das Ersetzen des Zertifikats finden Sie unter „Konfigurieren von SSL-Zertifikaten für View Server“ im Dokument *Installation von View*.

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

Hinweis Um die CA-signierten SSL-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, zu einem RDS-Desktop oder zu 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. auf einen RDS-Desktop und auf Anwendungen zuzugreifen, die auf diesem RDS-Host gehostet werden.

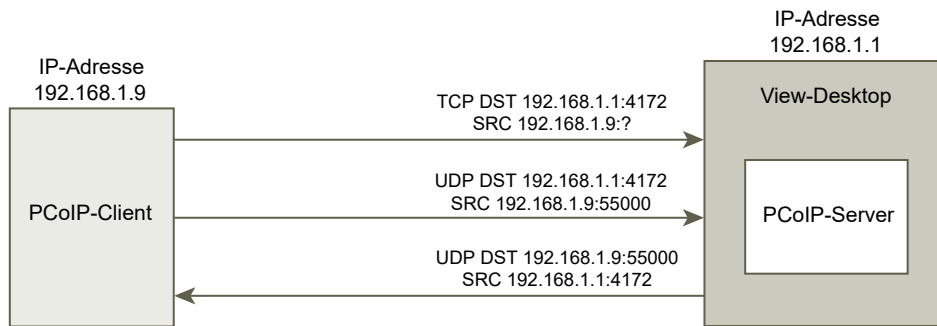
Verwenden der Netzwerkadressübersetzung (NAT) und Portzuordnung

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

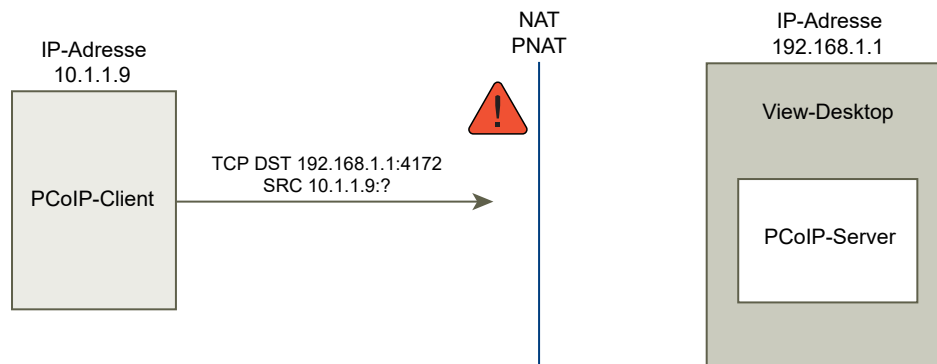
In den hier enthaltenen Beispielen müssen Sie die externen Adressierungsinformationen auf dem Desktop konfigurieren, sodass Horizon Client diese Informationen zum Herstellen einer Verbindung zum Desktop verwenden kann, indem NAT oder ein Portzuordnungs-Gerät verwendet wird. Dieser URL ist mit den Einstellungen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

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

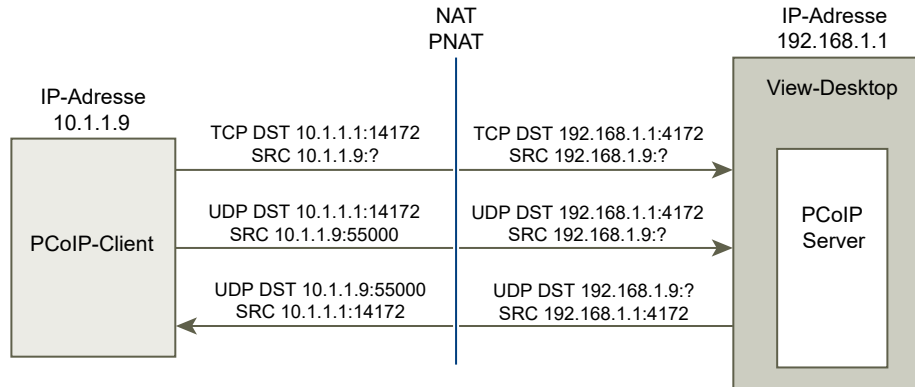
Wenn Sie ein NAT-Gerät zwischen dem Client und dem Desktop hinzufügen, sodass sie in einem anderen Adressbereich betrieben werden, und keine Konfigurationsänderungen am Plug-In durchführen, werden die PCoIP-Pakete nicht ordnungsgemäß umgeleitet und schlagen fehl. In diesem Beispiel verwendet der Client einen anderen Adressbereich und verfügt über die IP-Adresse 10.1.1.9. Das Setup schlägt fehl, weil der Client die Adresse des Desktops verwendet, 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` als 10.1.1.1 für diesen Desktop konfiguriert ist, gewährt das Plug-In dem Client die IP-Adresse 10.1.1.1, 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-Zielpartnummer 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.

Einrichten von HTML Access

Das VADC-Plug-In (View Agent Direct-Connection) unterstützt HTML Access auf VM-basierte Desktops. HTML Access auf RDS-Desktops oder -Anwendungen wird nicht unterstützt.

Dieses Kapitel enthält die folgenden Themen:

- [Installieren von View Agent für HTML Access](#)
- [Einrichten der statischen Inhaltsübermittlung](#)
- [Einrichten eines von einer vertrauenswürdigen Zertifizierungsstelle signierten SSL-Serverzertifikats](#)

Installieren von View Agent für HTML Access

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

Voraussetzungen

- Laden Sie die View Agent-Installationsdatei von der VMware-Produktseite unter <http://www.vmware.com/products/> 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 View Agent über die Befehlszeile und legen Sie einen Parameter fest, der View veranlasst, sich nicht beim View-Verbindungsserver zu registrieren.

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

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

Nächste Schritte

Weitere Informationen zur Installation des Plug-Ins „View Agent Direct-Connection“ finden Sie unter [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 View HTML Access von der VMware-Produktseite 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 Kopieren Sie VMware-Horizon-View-HTML-Access-y.y.y-xxxxxx.zip in einen temporären Ordner.
- 17 Entzippen Sie die Datei VMware-Horizon-View-HTML-Access-y.y.y-xxxxxx.zip.
Das Ergebnis ist eine Datei mit dem Namen portal.war.
- 18 Benennen Sie portal.war in portal.zip um.
- 19 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.
- 20 Öffnen Sie den **Editor**.
- 21 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>
<meta HTTP-EQUIV="REFRESH" content="0; url=https://<IP address or DNS name of desktop>/portal/
webclient/index.html">
</HEAD>
```

Einrichten eines von einer vertrauenswürdigen Zertifizierungsstelle signierten SSL-Serverzertifikats

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

Voraussetzungen

- Ersetzen Sie das standardmäßige selbstsignierte SSL-Serverzertifikat durch ein von einer vertrauenswürdigen Zertifizierungsstelle signiertes SSL-Serverzertifikat. Siehe [Ersetzen des standardmäßigen selbst signierten SSL-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. Siehe hierzu „Konfigurieren des View-Verbindungsservers, Sicherheitsservers oder von View Composer für die Verwendung eines neuen SSL-Zertifikats“ im Dokument *Installation von View*.

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 (G_SZ) SslHash zu diesem Registrierungsschlüssel hinzu.
- 8 Setzen Sie den Wert SslHash auf den Wert **Thumbprint**.

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

4

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

Dieses Kapitel enthält die folgenden Themen:

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

RDS-Hosts

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

In einer View-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 View 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 View Agent finden Sie unter „Einrichten von RDS-Hosts (Remote Desktop Services)“ im Dokument *Einrichten von Desktop- und Anwendungspools in View*. Informationen zur Installation des VADC-Plug-Ins finden Sie unter [Kapitel 1 Installation des Plug-Ins „View Agent Direct-Connection“](#).

Hinweis Wenn Sie View Agent installieren, fragt das Installationsprogramm Sie nach dem Hostnamen oder der IP-Adresse des View-Verbindungservers, mit dem View 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 [Berechtigung für RDS-Desktops und Anwendungen](#).

Berechtigung für RDS-Desktops und Anwendungen

Sie müssen den betreffenden Benutzern Berechtigungen für RDS-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 RDS-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' anzeigen** 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, um einen Benutzer zum Starten einer Anwendung 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 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 KB-Artikel „Sammeln von Diagnoseinformationen für VMware View“ unter <http://kb.vmware.com/kb/1017939>.

Dieses Kapitel enthält die folgenden Themen:

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

Falsche Grafikkhardware 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 View Agent eine falsche Version von VMware Tools installiert wird.

Lösung

- ◆ Installieren Sie View 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-View Agent-Protokoll. TRACE- und DEBUG-Informationen sind im Protokoll standardmäßig nicht enthalten.

Problem

Das View 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 im View 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 aus dem View Agent und dem Plug-In. Suchen Sie nach `wsnm_xmlapi`, um die Plug-In-Protokollzeilen zu finden.

Wenn der View 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, 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
```